Aurorean™ Virtual Network

ANG-1000
User's Guide

Version 1.0

ENTERASYS
NETWORKS™

Notice

Enterasys Networks and its licensors reserve the right to make changes in specifications and other information contained in this document without prior notice. The reader should in all cases consult Enterasys Networks to determine whether any such changes have been made. The hardware, firmware, or software described in this manual is subject to change without notice.

IN NO EVENT SHALL Enterasys Networks AND ITS LICENSORS BE LIABLE FOR ANY INCIDENTAL, INDIRECT, SPECIAL, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING BUT NOT LIMITED TO LOST PROFITS) ARISING OUT OF OR RELATED TO THIS MANUAL OR THE INFORMATION CONTAINED IN IT, EVEN IF Enterasys Networks AND ITS LICENSORS HAVE BEEN ADVISED OF, KNOWN, OR SHOULD HAVE KNOWN, THE POSSIBILITY OF SUCH DAMAGES.

Enterasys Networks, Inc.
35 Industrial Way
Rochester, NH 03866-5005

Part Number: AVN-ANG1-R10
May 2001
Printed in the USA

The Enterasys Networks logo, Aurorean, Prescriptive Diagnostics Engine, RiverMaster, Intelligent Client Routing, TollSaver are trademarks of Enterasys Networks.

Microsoft, MS, and MS-DOS are registered trademarks and Windows, Windows 95, Windows 98, Windows NT, Windows 2000 Professional and Windows Millennium are trademarks of Microsoft Corporation in the USA and other countries.

Virtual Network Computing is a trademark of AT&T Laboratories Cambridge.

ActiveState, ActivePerl, and PerlScript are trademarks of ActiveState Tool Corp.

Other trademarks and trade names used in this publication belong to their respective owners.

Aurorean Virtual Network software includes the following third-party components:

> Commercial support for ActivePerl is available through PerlClinic at http://www.ActiveState.com. Peer support resources for ActivePerl issues can also be found at the ActiveState Web site under support at http://ActiveState.com/support/. The ActiveState Repository has a large collection of modules and extensions in binary packages that are easy to install and use. To view and install these packages, use the Perl Package Manager (PPM) which is included with ActivePerl. ActivePerl is the latest Perl binary distribution from ActiveState and replaces what was previously distributed as Perl for Win32. The latest release of ActivePerl as well as other professional tools for Perl developers are available from the ActiveState Web site.
>
> Gate Daemon software © 1995 The Regents of the University of Michigan. All rights reserved.
> Gate Daemon was originated and developed through release 3.0 by Cornell University and its collaborators.
>
> A DES implementation written by Eric Young © 1995-1997 Eric Young (eay@cryptsoft.com). All rights reserved.
>
> MD4 and MD5 implementation derived from the RSA Data Security, Inc. MD4 Message-Digest Algorithm and MD5 Message-Digest Algorithm © 1991-2, RSA Data Security, Inc. Created 1991. All rights reserved.
>
> ccp.c - PPP Compression Control Protocol © 1994 The Australian National University. All rights reserved.
>
> chap.c - Crytographic Handshake Authentication Protocol © 1991 Gregory M. Christy. All rights reserved.
>
> chap_ms.c - Microsoft MS-CHAP compatible implementation © 1995 Eric Rosenquist, Strata Software Limited (www.strataware.com). All rights reserved.
>
> fsm.c - {Link, IP} Control Protocol Finite State Machine © 1989 Carnegie Mellon University. All rights reserved.
>
> Routines to compress and uncompress TCP packets (for transmission over low speed serial lines) © 1989 Regents of the University of California. All rights reserved.
>
> Portions of the Aurorean Client Software are copyrighted to ICE Engineering, Inc. and licensed through a GNU public license. For more information, including access to the source code, visit their Web site at www.ice.com.

Federal Communications Commission (FCC) Notices

The Aurorean Network Gateway-100 complies with Title 47 Part 15, Subpart B of FCC Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operation.

Modifications or changes made to this device, and not approved by Enterasys Networks may void the authority granted by the FCC or other such agency to operate this equipment.

There are no user-repairable components in the Aurorean Network Gateway-1000.

Canadian Notices

This digital apparatus does not exceed the Class B limits for radio noise emissions from digital apparatus set out in the interference-causing equipment standard entitled “Digital Apparatus”, ICES-003 of the Department of Communications (Cet appareil numérique respecte les limites bruits radioélectriques applicables aux appareils numériques de Classe A prescrites dans la norme sur le matériel brouilleur: “Appareils Numériques”, NMB-003 édictée par le ministre des Communications).

NOTICE: The Industry Canada label identifies certified equipment. This certification means that the equipment meets certain telecommunications network protective, operational and safety requirements. The Department does not guarantee the equipment will operate to the user's satisfaction.

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. In some cases, the inside wiring associated with a single line individual service may be extended by means of a certified connector assembly. The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to certified equipment should be made by an authorized Canadian maintenance facility designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

Users should ensure for their own protection that the electrical ground connections of the power utility, telephone lines and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.

CAUTION: Users should not attempt to make such connections themselves, but should contact the appropriate electric inspection authority, or electrician, as appropriate.

UL Notices

The Aurorean Policy Server and Aurorean Network Gateway have been tested and found to comply with the UL 1950 Revision 3 regulation.

European Notices

The ANG-1000 has been tested and found to comply with the CISPR 22:1997 Class B regulation.

⚠ **ELECTRICAL HAZARD:** Only qualified personnel should perform installation procedures.

Important Safety Instructions

1) Read these instructions carefully. Save these instructions for future reference.

2) Follow all warnings and instructions marked on the product.

3) Unplug this product from the wall outlet before cleaning. Do not use liquid cleaners or aerosol cleaners. Use a damp cloth for cleaning.

4) Do not use this product near water.

5) Do not place this product on an unstable cart, stand, or table. The product may fall, causing serious damage to the product.

6) Slots and openings in the chassis are provided for ventilation; to ensure reliable operation of the product and to protect it from overheating, these openings should not be blocked or covered. The openings should never be blocked by placing the product on a bed, sofa, rug, or other similar surface. This product should never be placed near or over a radiator or heat register, or in a built-in installation unless the proper ventilation is provided.

7) This product should be operated from the type of power indicated on the marking label. If you are not sure of the type of power available, consult Enterasys Networks or your local power company.

8) Do not allow anything to rest on the power cord. Do not locate this product where persons will walk on the cord.

9) If an extension cord is used with this product, make sure that the total ampere rating of the equipment plugged into the extension cord does not exceed the extension cord ampere rating. Also, make sure that the total rating of all products plugged into the wall outlet does not exceed the fuse rating.

10) Never push objects of any kind into this product through chassis slots as they may touch dangerous voltage points or short out parts that could result in a fire or electric shock. Never spill liquid of any kind on the product.

11) Do not attempt to service this product yourself, as operating or removing covers may expose you to dangerous voltage points or other risks. Refer all servicing to qualified service personnel.

12) Unplug this product from the wall outlet and refer servicing to qualified service personnel under the following conditions:

    a) When the power cord or plug is damaged or frayed.

    b) If liquid has been spilled into the product.

    c) If the product has been exposed to rain or water.

    d) If the product does not operate normally when the operating instructions are followed. Adjust only those controls that are covered by the operating instructions since improper adjustment of other controls may result in damage and will often require extensive work by a qualified technician to restore the product to normal condition.

    e) If the product has been dropped or the chassis has been damaged.

    f) If the product exhibits a distinct change in performance, indicating a need for service.

13) Use only the proper type of power supply cord set (provided in your accessories box) for this unit. It should be a detachable type, UL listed/CSA certified, type SPT-2, rated 7A 125V minimum, VDE approved or equivalent. Maximum length is 15 feet (4.6 meters).

Table of Contents

About This Guide

Chapter 1 – Overview

Chapter 2 – Installation

Chapter 3 – Configuring the ANG-1000 with Aurorean Web Config

Appendix A – Glossary

Appendix B – Specifications

Appendix C – Pin Assignments

Appendix D – License Agreement & Support

Index

About This Guide

This guide describes how to mount, connect, power-up, and maintain an Aurorean™ Network Gateway-1000 (ANG-1000) from Enterasys Networks.

This guide is written for administrators who want to configure the ANG-1000 for their remote clients or experienced users who are knowledgeable of basic networking principles.

Contents of the Guide

Information in this guide is arranged as follows:

- ❒ *Chapter 1, Overview* highlights the key features of the Aurorean Virtual Network family of enterprise VPN products.
- ❒ *Chapter 2, Installation* describes how to physically mount, connect, and power-up Aurorean servers.
- ❒ *Chapter 3, Configuring the ANG-1000 with Aurorean Policy Manager,* details how to configure the server.
- ❒ *Appendix A, Glossary* defines terms used in this manual.
- ❒ *Appendix B*, *Specifications* provides essential physical and operational characteristics of the ANG-1000.
- ❒ *Appendix C, Pin Assignments* describes the pinouts of the LAN connectors.
- ❒ *Appendix D, License Agreement & Support* describes the warranty terms and support policies covering Enterasys Networks products.

Conventions Used in This Guide

The following conventions are used in this guide:

☑ **NOTE**	Notes supply additional helpful information, provide a cross-reference to the source of more information, or emphasize issues you should consider when performing an action.
⚠ **CAUTION**	Cautions contain directions that can prevent you from damaging the product or losing data.
⚡ **WARNING**	Warnings provide directions that you must follow to avoid harming yourself.
Bold	Text in boldface indicates values you type using the keyboard or select using the mouse (for example, **a:\setup**). Default settings may also appear in bold.
Italics	Text in italics indicates a variable, important new term, or the title of a manual.
SMALL CAPS	Small caps specify the keys to press on the keyboard; a plus sign (+) between keys indicates that you must press the keys simultaneously (for example, CTRL+ALT+DEL).
`Courier font`	Text in this font denotes a file name or directory.

Related Publications

The following publications are also available with the Aurorean Network Gateway-1000:

- ❐ The *ANG-1000 Quick Setup* card which highlights the basic steps required to install the Aurorean Network Gateway-1000.
- ❐ The *Installation & Service Guide* which describes how to install and maintain the ANG-3000/7000 series, the Aurorean server which can be used to complete a VPN connection with the ANG-1000.
- ❐ A *Portable Document File (PDF)* version of this manual is available and can be downloaded from the Enterasys.com Web site. You can view this manual on-line or print a copy of it using Adobe Acrobat Reader 3.0 (or later). Acrobat Reader can be downloaded from the Enterasys web site or the Adobe web site at `www.adobe.com`.

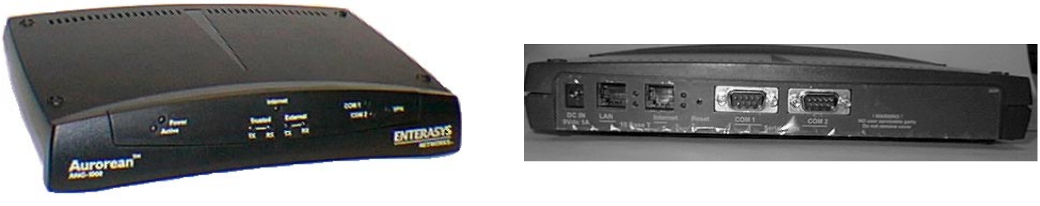
1

Overview

This chapter describes the key features of the Aurorean Network Gateway 1000 and how it is used.

System Description

The ANG-1000, displayed in Figure 1, provides home or small office connectivity to a corporate branch office or headquarters. It supports up to 25 tunnels.



ANG-1000
Front

ANG-1000
Rear

Figure 1 ANG-1000 Front and Rear Views

Figure 2 illustrates how the ANG-1000 typically connects to the corporate network.

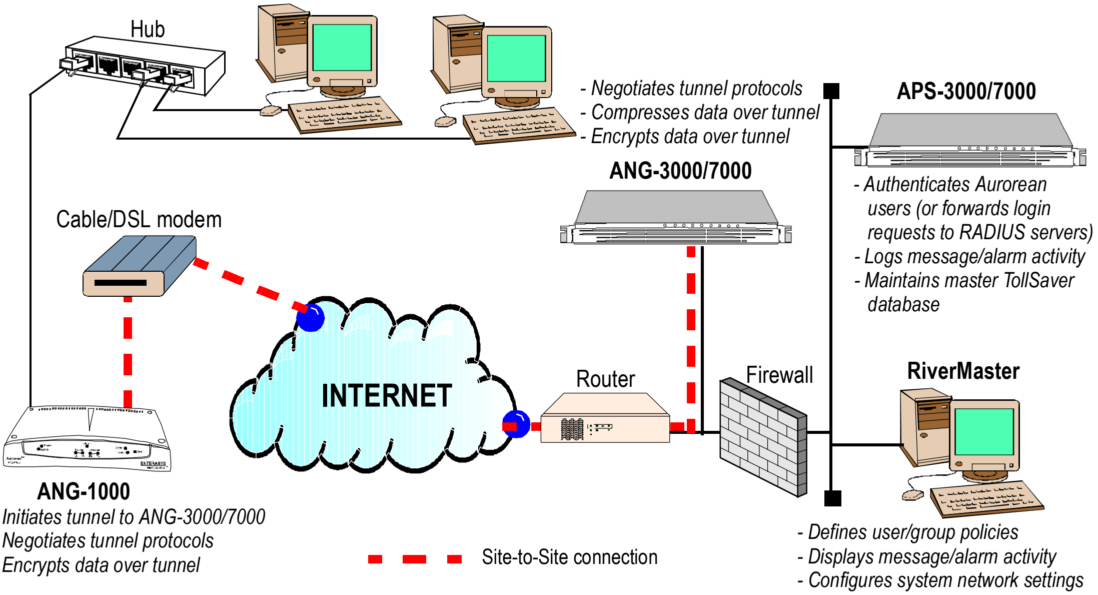

Hub
- Negotiates tunnel protocols
- Compresses data over tunnel
- Encrypts data over tunnel
ANG-3000/7000
APS-3000/7000
- Authenticates Aurorean users (or forwards login requests to RADIUS servers)
- Logs message/alarm activity
- Maintains master TollSaver database
Cable/DSL modem
INTERNET
Router
Firewall
RiverMaster
ANG-1000
- Initiates tunnel to ANG-3000/7000
- Negotiates tunnel protocols
- Encrypts data over tunnel
Site-to-Site connection
- Defines user/group policies
- Displays message/alarm activity
- Configures system network settings

Figure 2 ANG-1000 Topology

An ANG-1000 comes equipped with the following:

- ❒ 100-240V 47-63 Hz power supply.
- ❒ High-performance CPU: 91.5 MHz.
- ❒ Complete set of diagnostic LEDs that show the server's operational status.
- ❒ Two 10 Base-T Ethernet ports to connect the system to the network and the Internet.

2

Installation

This chapter describes the steps required to unpack, install and connect an Aurorean Network Gateway-1000 onto a desktop.

Unpacking the ANG-1000

Remove the ANG-1000 from the shipping box. Save the box in case the unit needs to be returned.

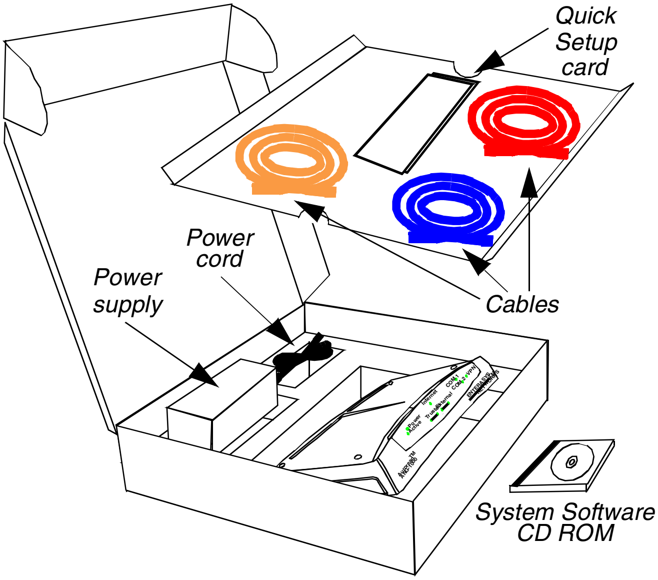


Figure 3 Removing ANG-1000 from the Shipping Box

The box contains a CD ROM with this instruction manual in the Adobe PDF format, a *Quick Setup* card and accessories.

Accessories

The ANG-1000 also is shipped with the following accessories:

- Two 10baseT cables (blue and orange) to connect to the LAN ports/hub.
- One cross-over (red) cable for a direct PC/Network Gateway connection.
- One power supply with an attached cable to connect to the ANG-1000.
- One power cord to connect the power supply to the AC outlet.

Location Planning

Place the ANG-1000 on a desktop near the following:

- Ethernet wall jack, patch panel, or hub with available ports.
- Near a DSL or Cable modem.
- A grounded wall outlet or uninterruptible power supply (UPS).

Connecting Cables

Ethernet cables are used to connect the ANG-1000 to your computer or LAN and the Internet.

ANG-1000 Front **ANG-1000 Rear**

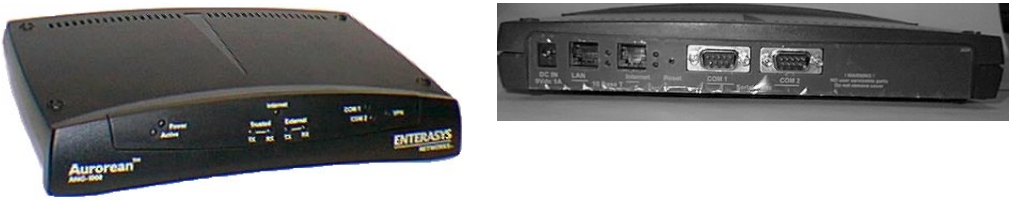


Figure 4 Front and Rear Views of the ANG-1000

All interconnections are made at the back of the ANG-1000 (refer to Figure 4). Although there is no power switch, a reset button is located in the rear of the unit.

CAUTION

If you press the reset button after you have configured your ANG-1000, you will lose your entire configuration. Any settings you supplied must then be re-entered. We strongly recommend that you do not use the reset button unless you want the configuration to return to factory defaults.

Ethernet Cables

The ANG-1000 is equipped with two 8-pin modular RJ-45 Ethernet ports labeled *Trusted* and *External* as shown in Figure 5. The Trusted port is connected to a computer or hub/switch with networked computers. The External port is connected to a cable or DSL modem.

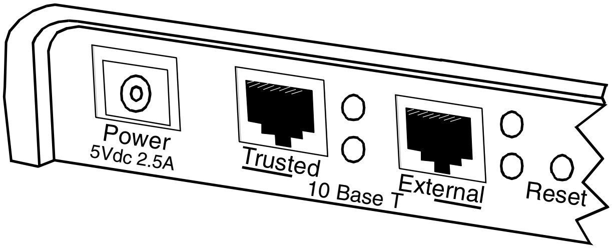


Figure 5 Location of the Ethernet Ports

The trusted connection can be either a sole desktop computer or a hub that connects up to 25 tunnels to the network as shown in Figure 6.

Connecting an ANG-1000

The ANG-1000 is typically set up in the configuration shown below.

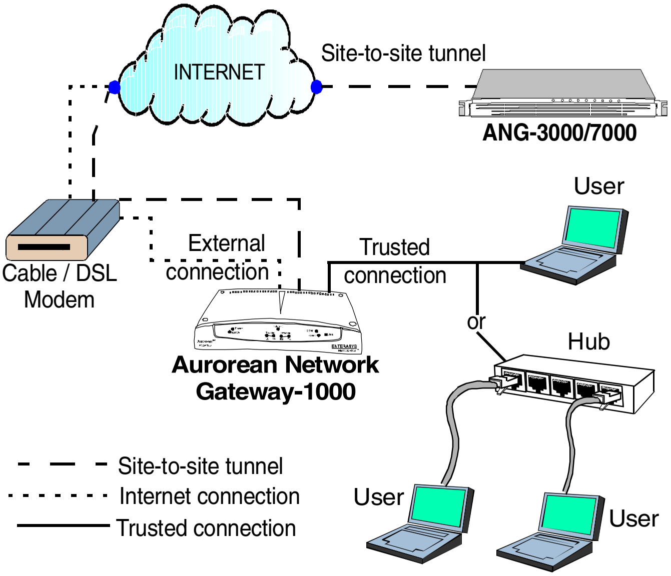


Figure 6 Connecting the ANG-1000

To connect the ANG-1000 Ethernet port, perform the following steps:

1. Do one of the following as shown in Figure 7:
   - If you are connecting to a *hub*, plug the blue, straight-through Ethernet cable into the Trusted port of the ANG-1000.
   - If you are connecting directly to a *computer*, attach one end of the red, cross-over cable to the Trusted port and the other end to an RJ45 connector on your computer. Skip to Step 3.

2. Plug the opposite end of the blue Ethernet cable into a wall jack, patch panel, or hub linked to a protected network segment.

   The top link LED next to the ANG-1000's Trusted port will immediately light if the port is connected to a 10 Mbps network *after* the unit is powered up.

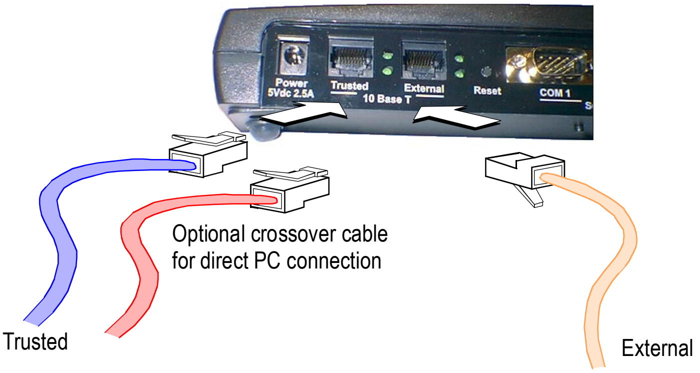


Figure 7 Connecting Ethernet Cables to an ANG-1000

3 Plug an orange, straight-through Ethernet cable into the External port as shown in Figure 7.

4 Plug the opposite end of this cable into a DSL or cable modem.

After you connect power, the top External LED at the rear of the ANG-1000 will be lit the moment the cable it is connected.

NOTE

If you have a DSL modem, you will need to get an IP address from your provider and configure it before the External LED will light. This condition may also exist for selective cable customers. Some cable internet providers require that you supply the MAC address of your computer. Refer to Chapter 3 for directions.

Connecting Power to the ANG-1000

WARNING

To avoid electrical shock, connect the Aurorean system only to a grounded (earthed) outlet.

A switching power supply including a 6′ power cord and a 7′ electrical cord with an attached power supply is supplied with each system. To connect these items to an ANG-1000, perform the following steps:

1 Plug the power supply cord into the system's power socket as shown in Figure 8.

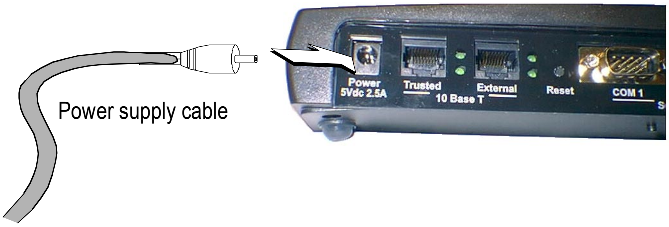


Figure 8 Connecting AC Power on the ANG-1000

2 Plug the correct end of the AC power cord into the power supply and the other end into a grounded AC outlet or UPS as shown in Figure 9.

The front Power LED will light the moment you power up the unit.

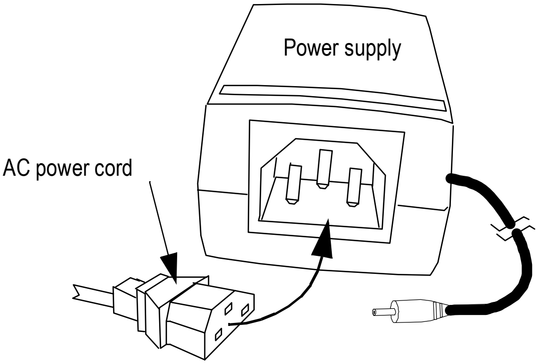


Figure 9 Connecting the Power Cable to the Power Supply

NOTE

International customers may swap the electrical cord segment shipped with the ANG-1000 for a cord that meets the proper standard for their country. A custom cord can be inserted in the power supply.

Checking ANG-1000 Connections

The ANG-1000 is now connected and ready for configuration. Check rear and front LEDS in the manner described below to confirm that the connections are working properly.

Rear Panel Link LEDs

The two top link LEDs on the rear panel light the moment a connection is made to the respective network. The two bottom link LEDs light when data is received and transmitted to the respective network by the ANG-1000. Trusted and external connections are operational and traffic is being passed as shown in Figure 10.

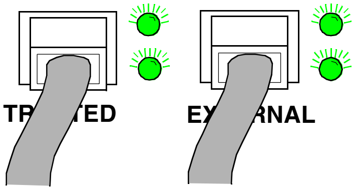


Figure 10 Network Connection Indicators

Front Panel LEDs

The two front LEDs behave as follows at when powered up at startup:

- ❒ Power LED lights
- ❒ Active LED blinks indicating the CPU is active

All front panel LEDs are displayed in Figure 11.

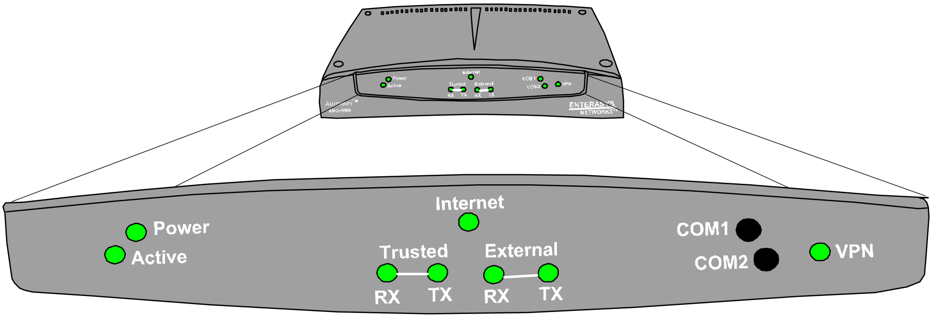


Figure 11 ANG-1000 Front Panel

After the ANG-1000 is configured and in use, the Internet, VPN, RX and TX LEDs will light and/or blink. Refer to Figure 12 for behavior of the LEDs.

The ANG-1000 is now ready for configuration. Refer to Chapter 3 for detailed instructions.

Power	●	*On when ANG is powered up*
Active	●	*Blinks when CPU is active*
Internet	●	*On when External network is assigned an IP address*
VPN	●	*On when a tunnel is connected*
TX	●	*Blinks when data is transmitted*
RX	●	*Blinks when data is received*

Figure 12 ANG-1000 Front Panel LEDs

NOTE

COM1 and COM2 LEDS are not operational at this time.

3

Configuring the ANG-1000 with Aurorean Web Config

To configure the ANG-1000, use the Internet browser on your computer and connect to the server via the Web. During the Web session, you run the Aurorean Web Config utility and configure the system. Figure 13 illustrates the process.

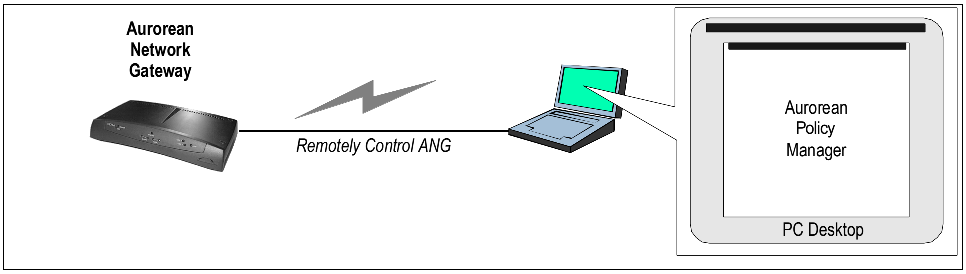


Figure 13 Configuring the ANG-1000 via Aurorean Web Config

Before You Begin

Before you begin configuration with Web Config, review the following:

❒ Be sure the ANG-1000 is cabled correctly as described in “Connecting an ANG-1000” in Chapter 2 of this manual.

❒ Ask your DSL or cable modem Internet provider and Network Administrator for any IP addresses, work group, network browsing or other information you may need to configure the ANG-1000 properly. Minimally, you will need:

  – The IP address of the ANG-3000/7000 you will connect to for setting up the VPN.

- To configure your PC to include the domain of the corporate network you will connect to.

  To do so on your Windows 95/98/ME/2000 desktop: click Start, select Settings and double-click Control Panel (Win 2000: Network and Dial-up Connections). Double-click the Network icon (Win 2000: right click on Local Area Connection and click Properties), click the Protocols tab, select TCP/IP Protocol, click Properties, select the DNS tab and add the Domain Suffix in the field provided. Click OK twice to close the open windows.

❐ On your computer, release and renew the IP address for all adaptors bound to TCP/IP. Refer to the Caution on page 24 for instructions.

❐ If you have cable service, learn the MAC address of your computer as described on page 32.

❐ If your computer was supplied a static IP address and Gateway by your service provider, you *must* now accept the address from a DHCP server and remove the gateway for the ANG-1000 to find and connect with the PC.

To do so, click Start, select Settings and double-click on Control Panel. Double-click the Network icon, select the Protocols tab and TCP/IP Protocol, click on Properties and the IP Address tab. Select the Obtain an IP address from a DHCP server radio button. Click Advanced, select the Gateway, click Remove and OK. Click OK twice more to close the open windows.

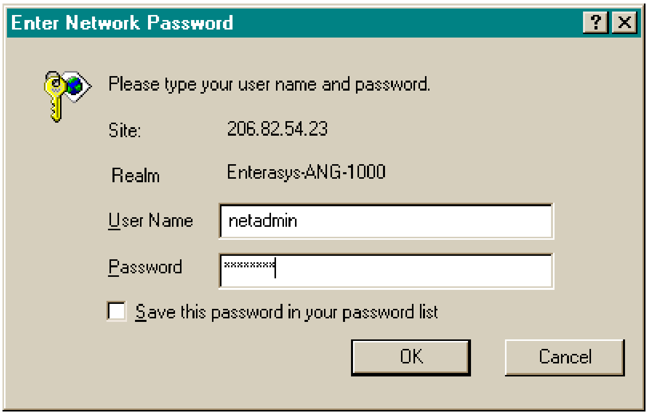
❐ Web Config supports the use of Internet Explorer 5 or Netscape 4 Web browsers.

Logging into Web Config

To log into Web Config, perform the steps below.

1. Point your Web browser at the default trusted IP address of the ANG-1000. In the browser's Location field at the top of the window, type: **http://192.168.1.1** or **aurorean.** (include the dot) and click OK.

   The Login window appears as shown in Figure 14.



Please type your user name and password.

Site: 206.82.54.23

Realm Enterasys-ANG-1000

User Name: netadmin

Password: ********

☐ Save this password in your password list

Figure 14 Login Window

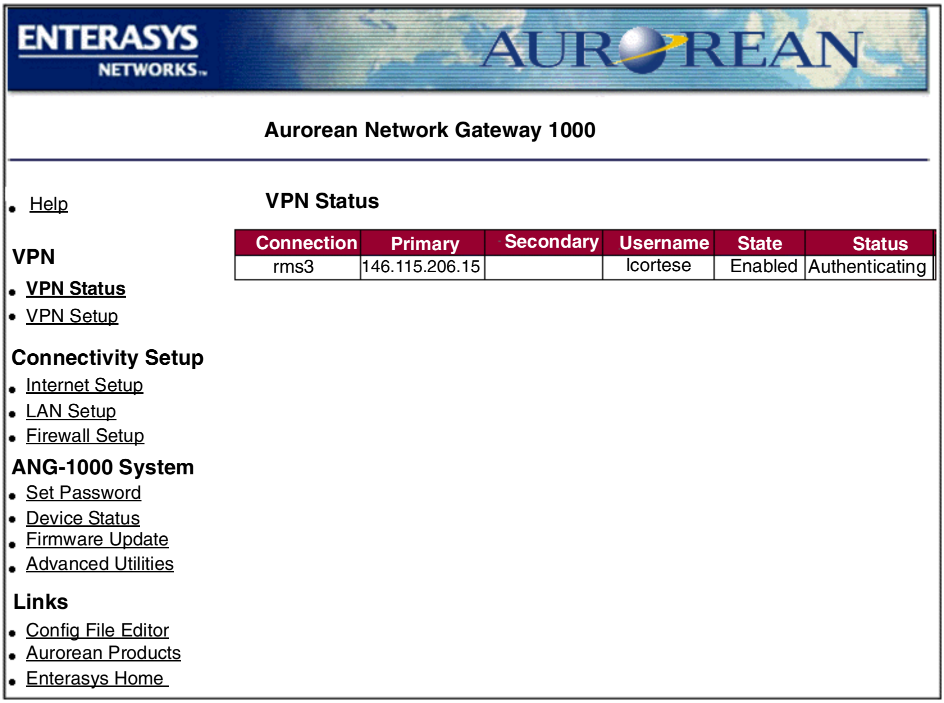
2. Type **netadmin** in the User Name and Password fields as shown in Figure 14.

3. Click the checkbox to save your password if you desire and click OK.

   The VPN Status window appears as shown in Figure 15.

Viewing VPN Status

The VPN Status window is the first screen to appear after logging in. At this point, you have just begun configuration so the VPN Status window appears empty. Later, after you have configured a VPN connection to an ANG-3000/7000, the window will display information similar to the data shown in Figure 15.



VPN Status

Connection	Primary	Secondary	Username	State	Status
rms3	146.115.206.15		lcortese	Enabled	Authenticating

Figure 15 VPN Status Window

1 Click the Firmware Upgrade menu option and go to the next page.

Downloading the Latest Firmware

After logging in, download the latest firmware image to the ANG-1000's flash memory (provided the MAC address is set for cable service users - refer to page 32) by accessing the FTP server where it is stored. As new firmware becomes available, you can update it again. Begin updating your firmware by performing the following steps:

1 Click the Firmware Upgrade menu option.

The Firmware Upgrade window appears as shown in Figure 16.

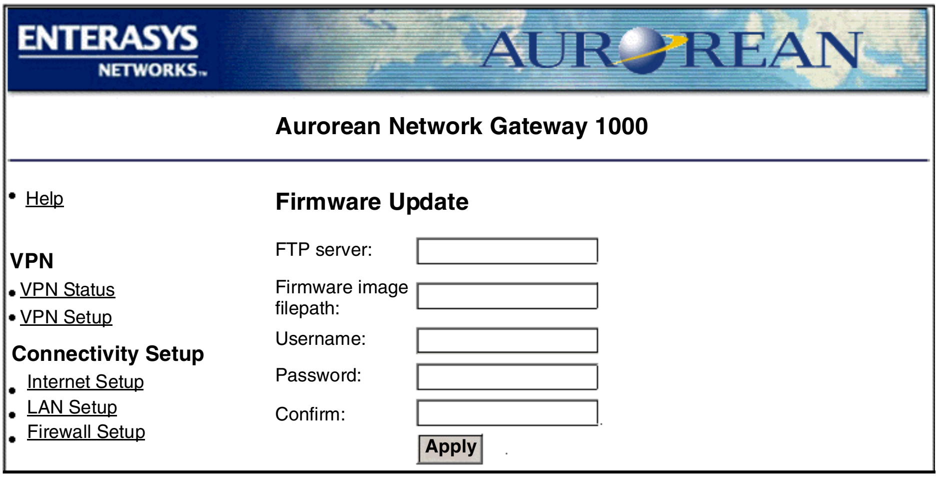


Figure 16 Firmware Update Window

2 In the FTP server field, enter the name of the FTP server where the new ANG image is stored: **ang.enterasys.com**.

3 Type the full path of the location of the Firmware image: **`/ang1000/ANG1000.bin`**

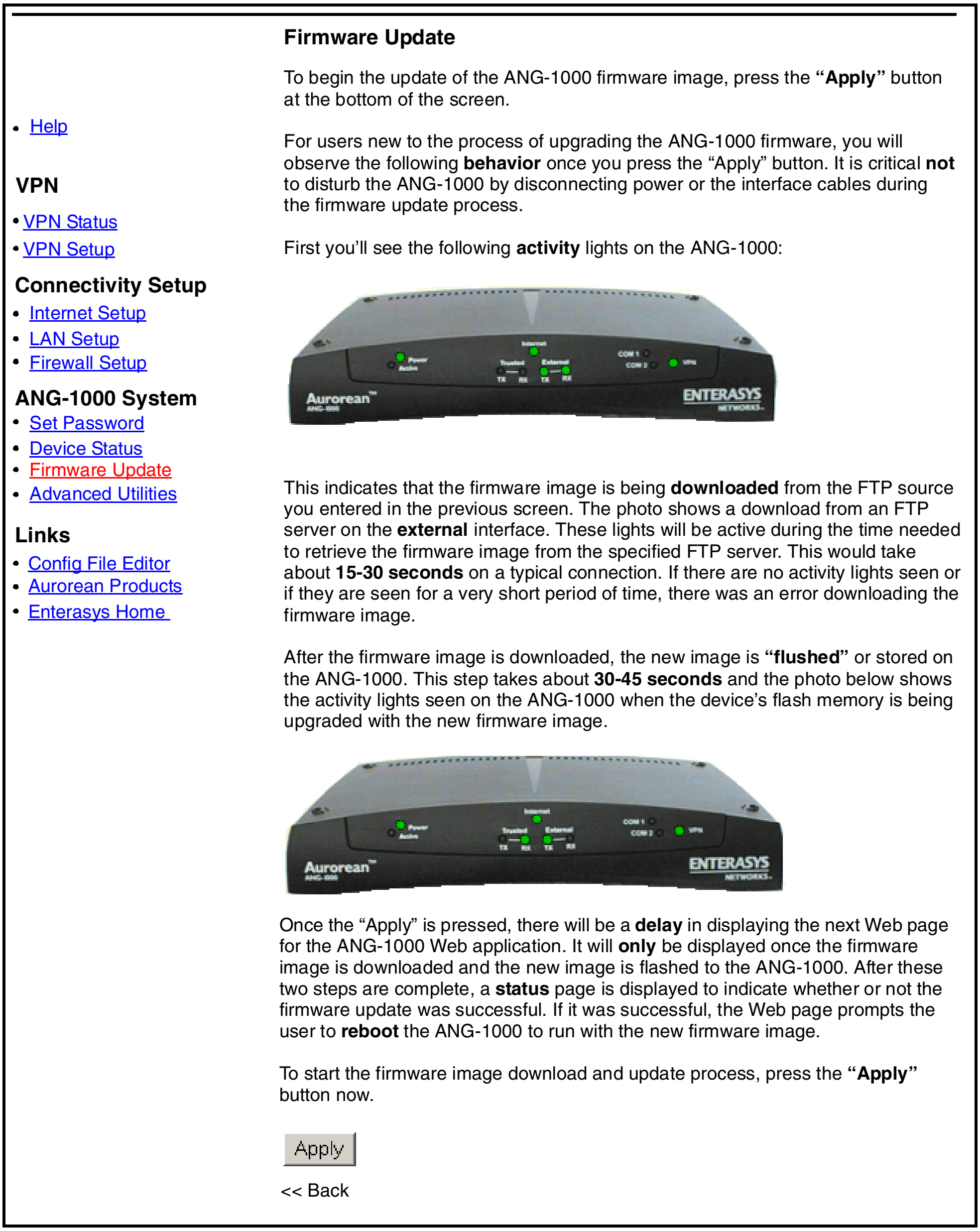
4 Enter the Username **anonymous**

5 Enter **netadmin** in the Password and Confirm fields and click Apply.

The Firmware Update window appears as shown in Figure 17.

6 Click Apply and watch the External/Trusted LEDs on the front panel blink displaying an inside/outside pattern.

The image is downloaded for15-30 seconds and loaded in flash memory for another 30-45 seconds. If the LEDs do not blink or only for a very short interval, the download failed and you must try again.



- Help

VPN

- VPN Status
- VPN Setup

Connectivity Setup

- Internet Setup
- LAN Setup
- Firewall Setup

ANG-1000 System

- Set Password
- Device Status
- Firmware Update
- Advanced Utilities

Links

- Config File Editor
- Aurorean Products
- Enterasys Home

Firmware Update

To begin the update of the ANG-1000 firmware image, press the “**Apply**” button at the bottom of the screen.

For users new to the process of upgrading the ANG-1000 firmware, you will observe the following **behavior** once you press the “Apply” button. It is critical **not** to disturb the ANG-1000 by disconnecting power or the interface cables during the firmware update process.

First you’ll see the following **activity** lights on the ANG-1000:

This indicates that the firmware image is being **downloaded** from the FTP source you entered in the previous screen. The photo shows a download from an FTP server on the **external** interface. These lights will be active during the time needed to retrieve the firmware image from the specified FTP server. This would take about **15-30 seconds** on a typical connection. If there are no activity lights seen or if they are seen for a very short period of time, there was an error downloading the firmware image.

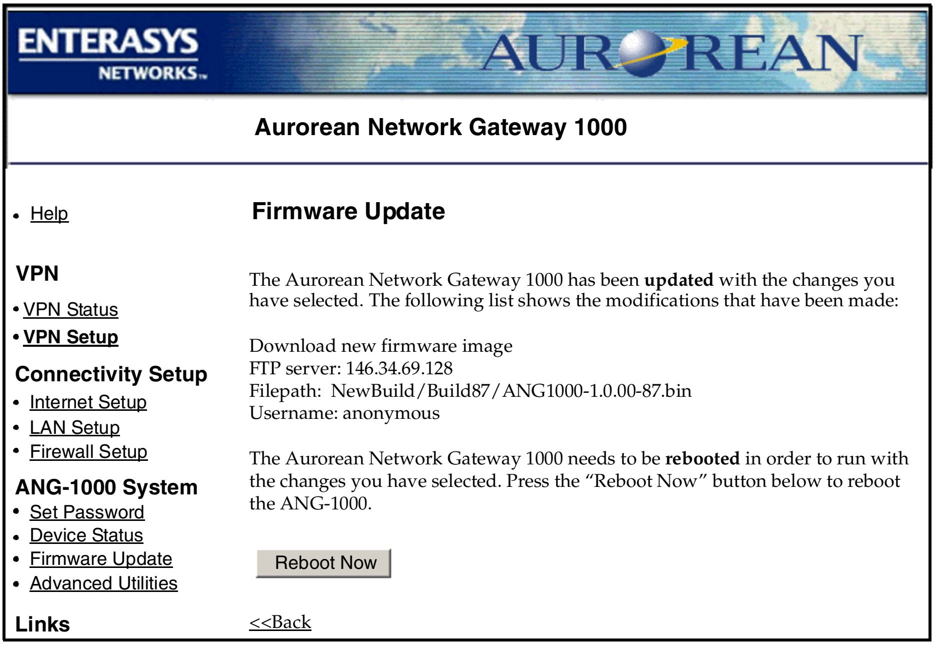
After the firmware image is downloaded, the new image is **“flushed”** or stored on the ANG-1000. This step takes about **30-45 seconds** and the photo below shows the activity lights seen on the ANG-1000 when the device’s flash memory is being upgraded with the new firmware image.

Once the “Apply” is pressed, there will be a **delay** in displaying the next Web page for the ANG-1000 Web application. It will **only** be displayed once the firmware image is downloaded and the new image is flashed to the ANG-1000. After these two steps are complete, a **status** page is displayed to indicate whether or not the firmware update was successful. If it was successful, the Web page prompts the user to **reboot** the ANG-1000 to run with the new firmware image.

To start the firmware image download and update process, press the “**Apply**” button now.

Figure 17 Second Firmware Update Window

7 After downloading and “flashing “are complete, a status page displays as shown in Figure 18 indicating the process was successful and displaying the FTP server IP address and new build filepath.



Aurorean Network Gateway 1000

Firmware Update

The Aurorean Network Gateway 1000 has been **updated** with the changes you have selected. The following list shows the modifications that have been made:

Download new firmware image
FTP server: 146.34.69.128
Filepath: NewBuild/Build87/ANG1000-1.0.00-87.bin
Username: anonymous

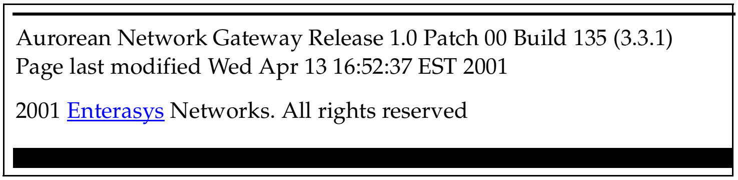
The Aurorean Network Gateway 1000 needs to be **rebooted** in order to run with the changes you have selected. Press the “Reboot Now” button below to reboot the ANG-1000.

Figure 18 Successful Firmware Update Window

8 Reboot the ANG-1000 by clicking Reboot Now.

The ANG-1000 will take a few moments to accept the new software.

9 To ensure that the image was updated, compare the date last modified, Release, Build and Patch numbers in the lower left corner of the VPN Status window as shown in Figure 15 with the previous release information. The Device Status window also lists this data.


Aurorean Network Gateway Release 1.0 Patch 00 Build 135 (3.3.1)
Page last modified Wed Apr 13 16:52:37 EST 2001

2001 Enterasys Networks. All rights reserved

Figure 19 Image Date and Build Information

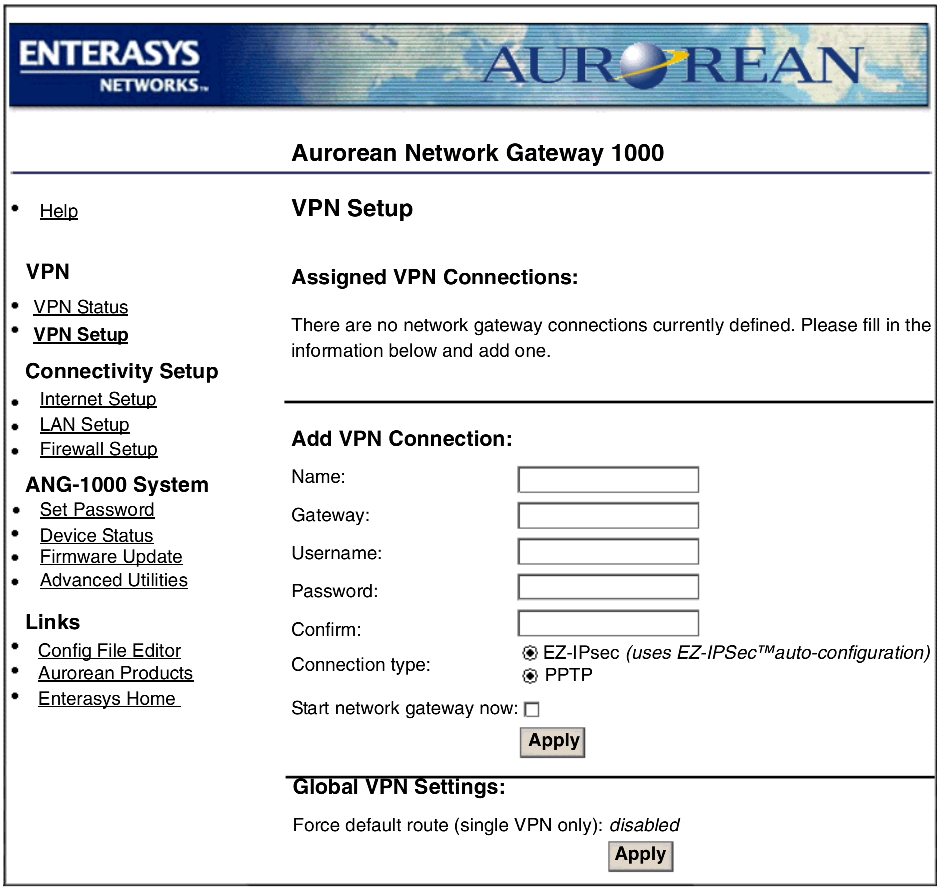
Setting Up the VPN

The VPN configuration created on the ANG-1000 completes a link with the ANG-3000/7000 on the remote end of this connection. If your network administrator has already set up the ANG-3000/7000 with appropriate User, Password and Group information, after setting up the VPN you will build the site-to-site tunnel connection and be up and running on the corporate LAN.

Begin VPN Setup by performing the following steps:

1 Click the VPN Setup menu option.

The VPN Setup window appears as shown in Figure 20.



Aurorean Network Gateway 1000

VPN Setup

Assigned VPN Connections:

There are no network gateway connections currently defined. Please fill in the information below and add one.

Add VPN Connection:

Name:

Gateway:

Username:

Password:

Confirm:

Connection type: ● EZ-IPsec *(uses EZ-IPSec™auto-configuration)* ● PPTP

Start network gateway now: □

Global VPN Settings:

Force default route (single VPN only): *disabled*

Figure 20 VPN Setup Window

1 Enter the Name of the remote ANG-3000/7000 you are connecting to.

2 Enter the Gateway IP address of the remote ANG-3000/7000.

3 Enter the Username on the remote ANG-3000/7000.

4 Enter the Password on the remote ANG-3000/7000.

5 Confirm the password on the remote ANG-3000/7000.

6 Select the Connection type: either EZ-IPsec or PPTP.

The EZ-IPsec feature provides one-button configuration for standard IPSec with IKE tunnels connecting to an ANG-3000/7000. Users of legacy RiverPilot Release 2.1 and 2.2 as well as users of the Aurorean Client Release 3.0 can upgrade to 3.1 without having to uninstall/reinstall their client software.

7 *Optional*. Click the Start network gateway now checkbox to create instant access or wait until the other end of the connection is created.

8 *Optional*. Click Force default route under Global VPN Settings.

Force default route disables the ANG-1000's Intelligent Client Routing (ICR) feature which allows users to browse the Internet outside the tunnel. Be aware that with Force Default enabled, the ANG-1000 transmits all traffic through the tunnel which may cause Web browsing problems. This feature works with only one tunnel up and running; it is disabled if you create more than one tunnel.

9 Click Apply.

After applying your changes, a VPN Setup update window appears displaying configuration revisions.

NOTE

Now that you have set up a site-to-site connection, configuration is complete unless you want to change the default Internet, LAN, Firewall, Password default values or your service is a Digital Subscriber Line (DSL) which requires that you set a PPPoE assigned IP address (refer to "Setting Up the Internet Connection" on page 20). Some cable internet providers also require that you specify a MAC address (refer to "Using Advanced Utilities" on page 31 for more information).

NOTE

If you press the reset button after you have configured your ANG-1000, you will lose your entire configuration. Any settings you supplied must then be re-entered. We strongly recommend that you do not use the reset button unless you want the configuration to return to factory defaults.

Setting Up the Internet Connection

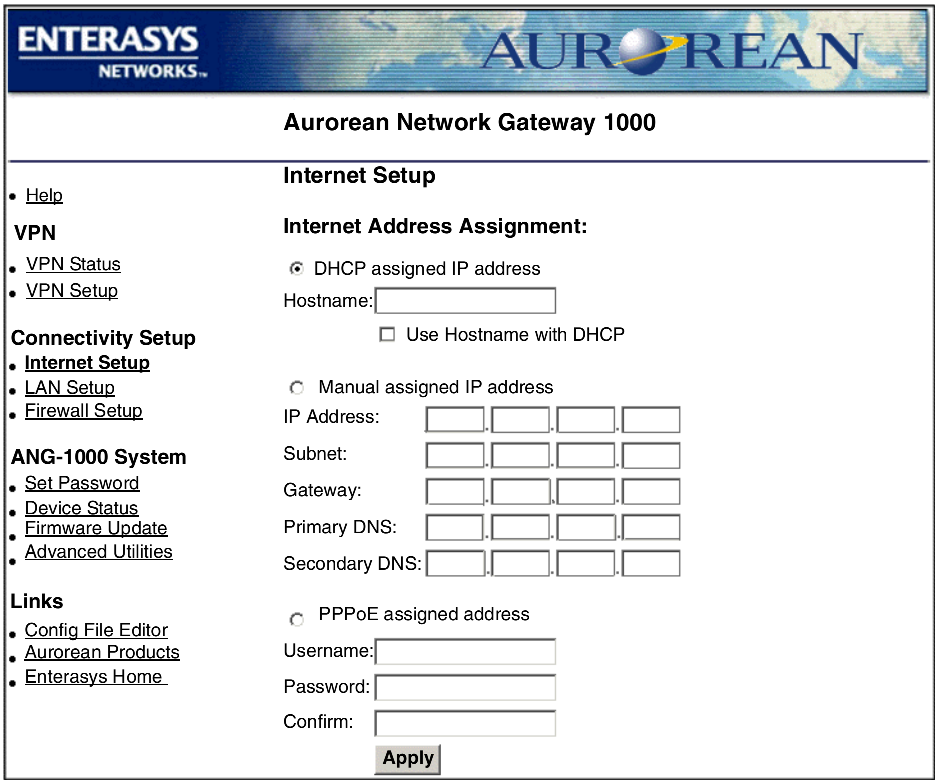
Internet configuration of the External side of the ANG-1000 involves choosing the type of IP address assignment the ANG-1000 will accept. The ANG can accept one of the following:

- ❒ A DHCP-assigned IP address - your network automatically sets the ANG's IP address via the DHCP (Dynamic Host Configuration Protocol) server.
- ❒ A Manual-assigned IP address - you or your network administrator set the ANG's IP address and associated Subnet, Gateway, and DNS values. Consult with your Network Administrator for required values.
- ❒ A PPPoE (PPP over Ethernet) assigned IP address - your DSL provider transparently sets the IP address via the use of a Username and Password. Obtain this information from your service provider before you enter this data.

Begin Internet Setup by performing the following steps:

1 Click the Internet Setup menu option.

The Internet Setup window appears as shown in Figure 21.



Aurorean Network Gateway 1000

- Help

VPN

- VPN Status
- VPN Setup

Connectivity Setup

- Internet Setup
- LAN Setup
- Firewall Setup

ANG-1000 System

- Set Password
- Device Status
- Firmware Update
- Advanced Utilities

Links

- Config File Editor
- Aurorean Products
- Enterasys Home

Internet Setup

Internet Address Assignment:

● DHCP assigned IP address

Hostname:

□ Use Hostname with DHCP

○ Manual assigned IP address

IP Address:

Subnet:

Gateway:

Primary DNS:

Secondary DNS:

○ PPPoE assigned address

Username:

Password:

Confirm:

Apply

Figure 21 Internet Setup Window

2 Do one of the following:

❒ Click the DHCP radio button and perform the following steps:

– Enter a Hostname for the system.

– *Optionally*, check the Use hostname with DHCP checkbox.

– Click Apply.

❒ Click the Manual assigned IP address radio button and perform the following steps:

– Specify the ANG-1000's IP address.

– Set the Subnet mask.

- Enter the Gateway IP address.
- Specify the Primary DNS IP address.
- Set the Secondary DNS IP address.
- Click Apply.

❒ Click the PPPoE assigned IP address radio button and perform the following steps:

- Specify a Username supplied by your cable/DSL provider.
- Enter a Password.
- Type the password again in the Confirm field.
- Click Apply.

3 If you chose the Manual or PPPoE options, a window appears detailing the reconfiguration changes and prompting you to reboot the ANG-1000. Click Reboot Now.

After a few moments when an IP address has been received for the external port, the Internet LED will turn on. If a static IP address was configured, the Internet LED will shine immediately.

NOTE

If you press the reset button after you have configured your ANG-1000, you will lose your entire configuration. Any settings you supplied must then be re-entered. We strongly recommend that you do not use the reset button unless you want the configuration to return to factory defaults.

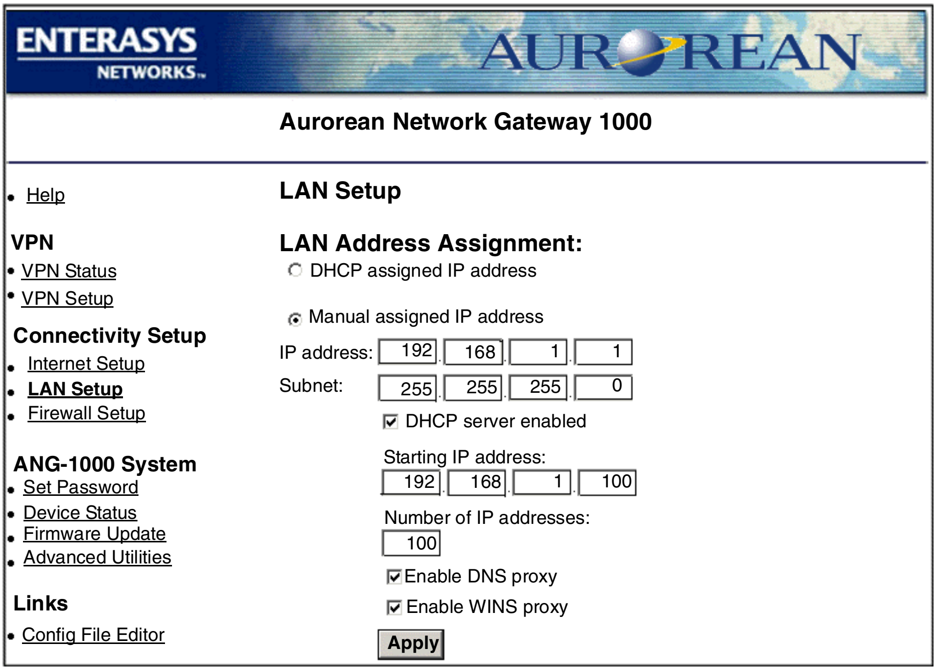
Setting Up the LAN

LAN configuration of the Trusted side of the ANG-1000 involves choosing either to manually set an IP address and subnet for the ANG-1000 or dynamically assigning its IP address via your network's DHCP server.

Begin LAN Setup by performing the following steps:

1 Click the LAN Setup menu option.

The LAN Setup window appears as shown in Figure 22.



Aurorean Network Gateway 1000

- Help

VPN
- VPN Status
- VPN Setup

Connectivity Setup
- Internet Setup
- **LAN Setup**
- Firewall Setup

ANG-1000 System
- Set Password
- Device Status
- Firmware Update
- Advanced Utilities

Links
- Config File Editor

LAN Setup

LAN Address Assignment:

○ DHCP assigned IP address

● Manual assigned IP address

IP address: 192 . 168 . 1 . 1

Subnet: 255 . 255 . 255 . 0

☑ DHCP server enabled

Starting IP address: 192 . 168 . 1 . 100

Number of IP addresses: 100

☑ Enable DNS proxy

☑ Enable WINS proxy

Apply

Figure 22 LAN Setup Window

2 Do one of the following:

❒ Click the DHCP assigned IP address radio button and perform the following steps:

– Click Apply.

❒ Click the Manual assigned IP address radio button and perform the following steps:

- Set the ANG-1000's IP address.
- Set the Subnet mask.
- *Optional*. Click the DHCP server enabled box if the server is up and running.
- Set the Starting IP address of the range of consecutive IP addresses you will create for this ANG-1000.
- Set the total Number of IP addresses the ANG-1000 can distribute.
- *Optional*. Keep Enable DNS proxy checked so that the ANG-1000 will act as a DNS server for all its tunnels. DNS proxy resolves host names and IP addresses because the domain server is non-routable, forcing attached hosts to request these values. If your hosts know the DNS address they are seeking, you can disable this feature. This option is on by default.
- *Optional*. Keep Enable WINS proxy checked so that PCs on the LAN can be notified of WINS servers discovered during tunnel setup. WINS proxy notifies local PCs of the remote WINS servers without manual intervention. This option can be disabled if local PCs already know remote WINS server IP addresses. This option is on by default.
- Click Apply.

CAUTION

If you change the default LAN Setup and reboot the ANG-1000, you must release and renew the IP address for all adaptors bound to TCP/IP on your connected computer(s) in order to reconnect with the ANG-1000 and make future changes. Perform the following steps:

- On your desktop, click Start. and Run.
- For Windows 95/98/ME systems, type: `winipcfg,` click OK, click Release and click OK. Then click Renew All and click OK.

- For Windows NT/2000 systems, type `ipconfig /release` and press ENTER. Then type `ipconfig /renew` and press ENTER.
- For Macintosh systems, check the TCP-IP control panel.

3 If you chose the DHCP option or changed the DNS or WINS default entries, a window appears detailing the reconfiguration changes and prompting you to reboot the ANG-1000. Click Reboot Now.

NOTE

If you press the reset button after you have configured your ANG-1000, you will lose your entire configuration. Any settings you supplied must then be re-entered. We strongly recommend that you do not use the reset button unless you want the configuration to return to factory defaults.

Setting Up the Firewall

Firewall security is established on the ANG-1000's Trusted interface by default. But, you may choose to permit unencrypted traffic over External or Trusted connections by disabling Web or Telnet access to them.

NOTE

Enabling any of the following options allows Web or Telnet traffic to run in the clear over the ANG-1000. You can permit the *transmission* of unencrypted traffic but the ANG-1000 will drop packets it *receives* outside the tunnel. We recommend that you allow Web and Telnet access on the LAN connection but disable these permissions on the Internet and VPN Gateway connections.

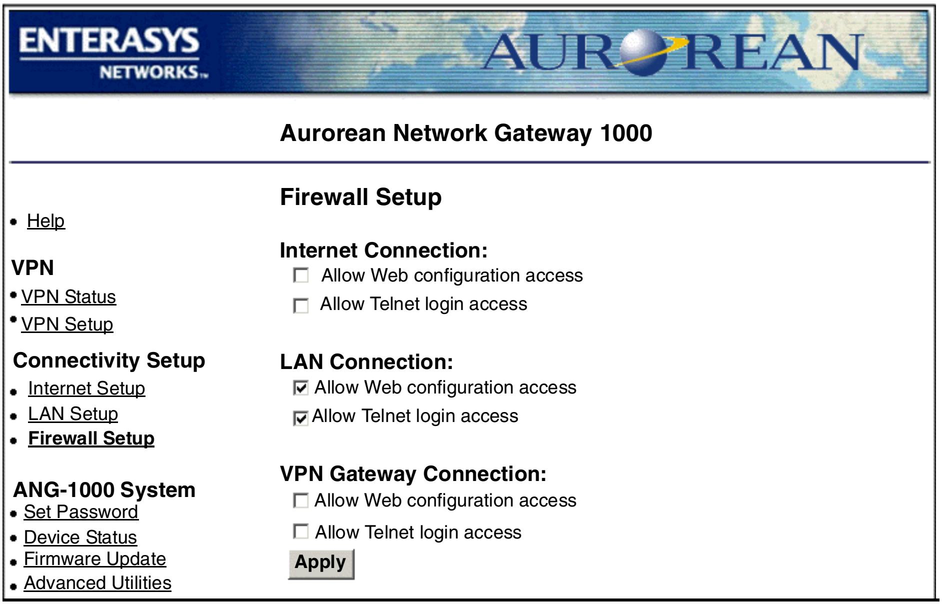
WARNING

If you leave all three connections disabled, you will be UNABLE TO CONFIGURE THE ANG-1000 without resetting the system.

Begin Firewall Setup by performing the following steps:

1 Click the Firewall Setup menu option.

The Firewall Setup window appears as shown in Figure 24.



Aurorean Network Gateway 1000

Firewall Setup

Internet Connection:
□ Allow Web configuration access
□ Allow Telnet login access

LAN Connection:
☑ Allow Web configuration access
☑ Allow Telnet login access

VPN Gateway Connection:
□ Allow Web configuration access
□ Allow Telnet login access

Figure 23 Firewall Setup Window

2 Enable the option of your choice and click Apply.

NOTE

Experienced administrators can fine tune firewall functionality by editing the *ipfwadm* file in the Configuration Editor. For more detailed information, check the following IPFWADM Web sites:
- www.xos.nl/linux/ipfwadm/paper/
- www.fwtk.org/ipfwadm/faq/ipfwadm-faq.html

NOTE

If you press the reset button after you have configured your ANG-1000, you will lose your entire configuration. Any settings you have changed from factory defaults, such as firewall rules, will be removed. We recommend that you save these settings to a Notepad file which you then can reference if you are compelled to use the reset button.

Setting Your Password

To further ensure security for your ANG-1000, you should configure a new password to replace the factory-installed password *netadmin*.

Change the Password by performing the following steps:

1 Click the Set Password menu option.

The Set Password window appears as shown in Figure 24.

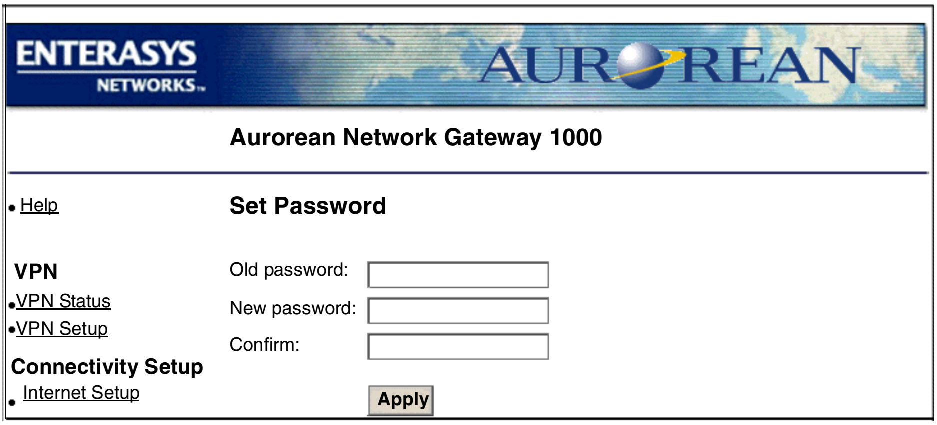


Figure 24 Set Password Window

2 Type the old Password in the field provided.

3 Type a new Password in the field provided.

4 Confirm the new password in the field provided.

5 Click Apply.

Checking Device Status

The Device Status window provides a host of important data to ensure the ANG-1000 is connected properly and to permit troubleshooting as problems occur. When consulting Enterasys Customer Support, you will be asked to display this window.

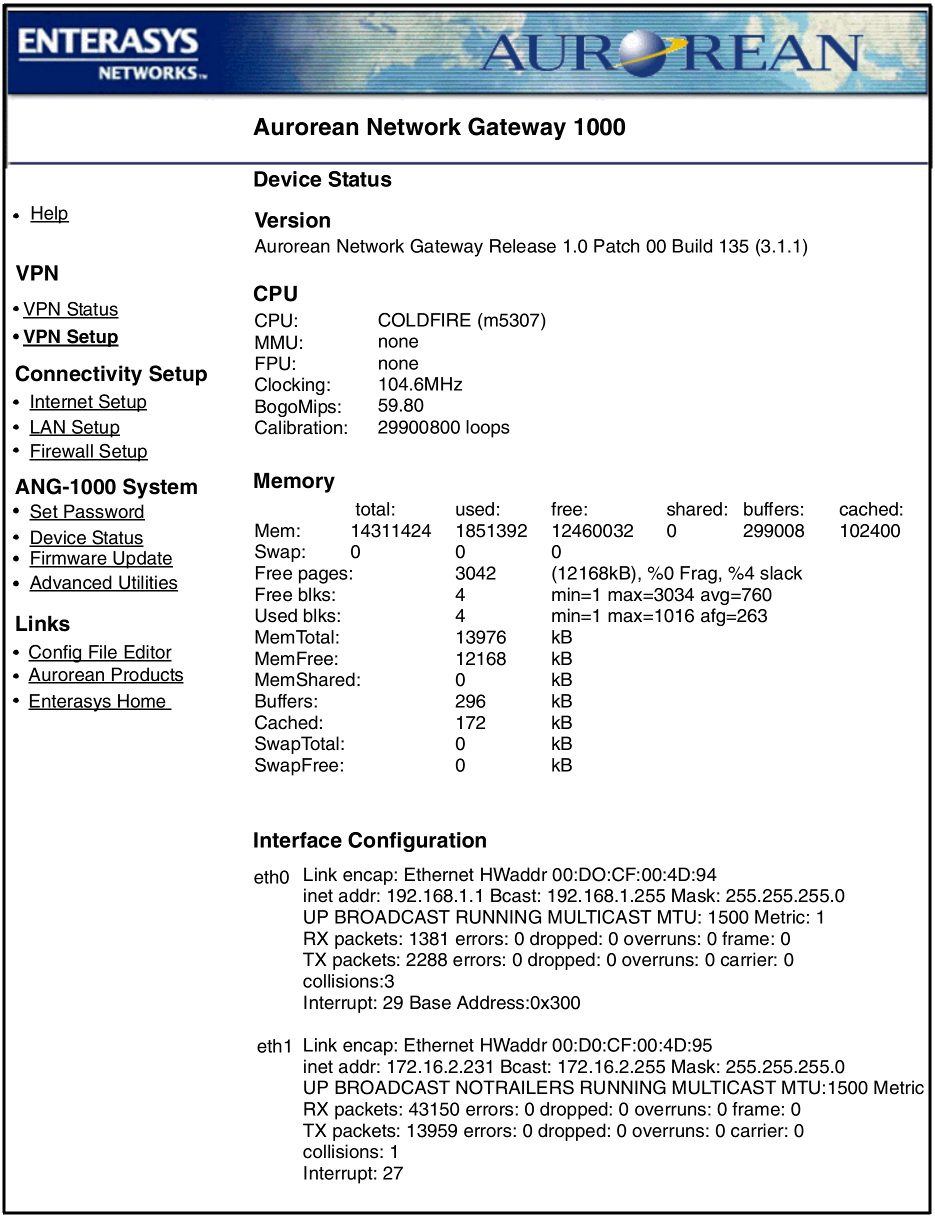
The following categories are detailed in the Device Status window:

- ❒ *Version* lists the Release, Patch and Build numbers, and internal name of the ANG-1000's firmware.
- ❒ *CPU* itemizes Motorola Coldfire chip specifications.
- ❒ *Memory* enumerates ANG-1000 memory values including Total, Used, Free, Shared, Cached, Buffered and Swapped bytes.
- ❒ *Interface Configuration* describes Trusted (eth0), External (eth1), IPsec (eth1:0-24), PPTP (ppp0-24) and Local Loopback (lo) port data including IP and MAC addresses, netmasks, Receive and Transmit errors and other information. Note that the ppp0 interface is the Internet, not WAN interface, if the Internet is configured for PPPoE.
- ❒ *Network Devices* tabulates interface Receive and Transmit errors.
- ❒ *Route Table* entries detail connected networks, gateways, their associated IP addresses, netmasks and other data.
- ❒ *Interrupts* lists the hardware interrupts supported on the ANG-1000 as well as their vectors and interrupt counters. The two SMC9194 items listed are the Ethernet Trusted and External port interrupts.
- ❒ *System Log* categorizes ANG-1000 functions/malfunctions including routing connections/disconnections.

Check Device Status by performing the following step:

1 Click the Device Status menu option.

The Device Status window appears as shown in Figure 25.



Aurorean Network Gateway 1000

Device Status

Version

Aurorean Network Gateway Release 1.0 Patch 00 Build 135 (3.1.1)

CPU

```
CPU:          COLDFIRE (m5307)
MMU:          none
FPU:          none
Clocking:     104.6MHz
BogoMips:     59.80
Calibration:  29900800 loops
```

Memory

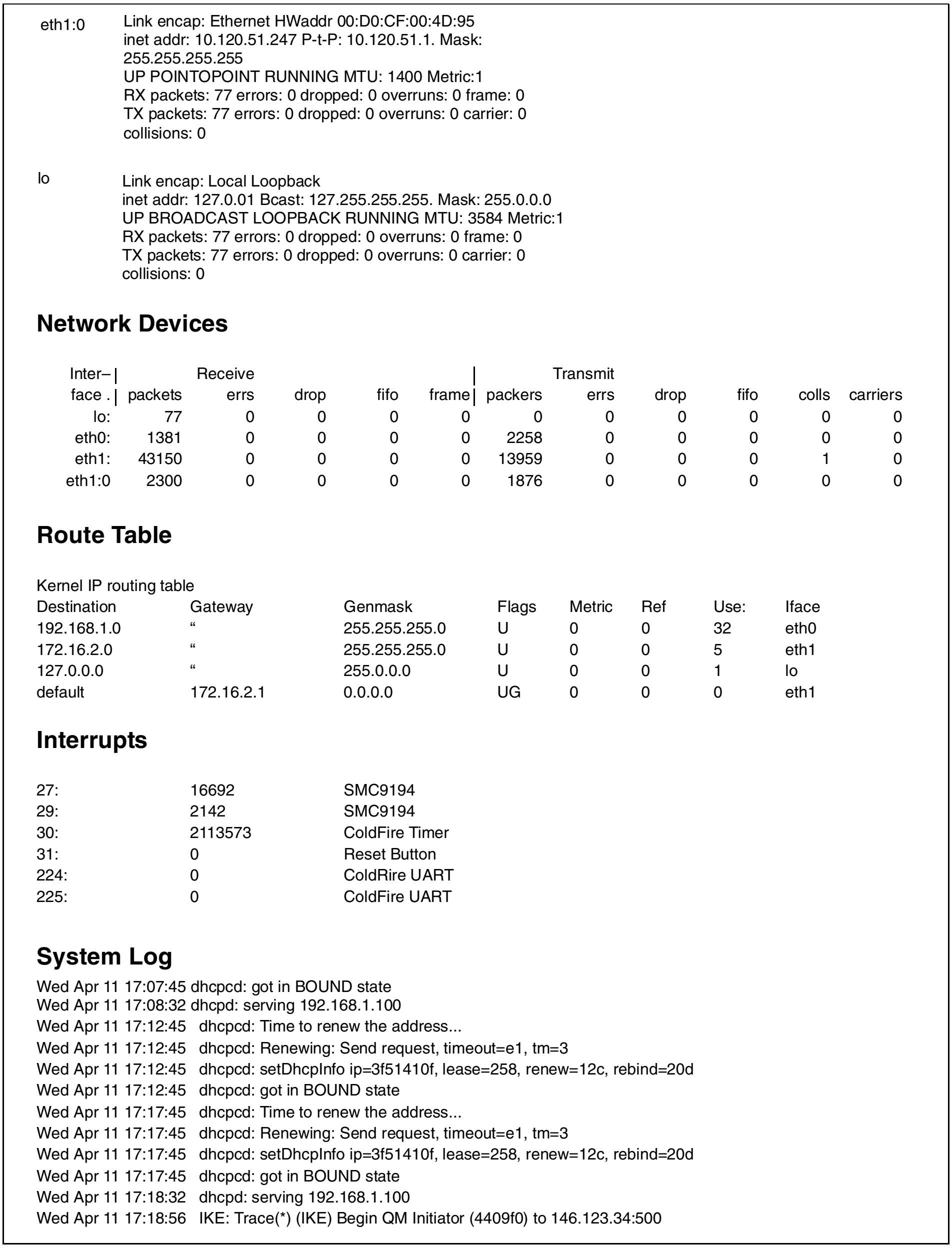
```
            total:      used:      free:         shared:   buffers:   cached:
Mem:       14311424    1851392    12460032      0         299008     102400
Swap:      0           0          0
Free pages:            3042       (12168kB), %0 Frag, %4 slack
Free blks:             4          min=1 max=3034 avg=760
Used blks:             4          min=1 max=1016 afg=263
MemTotal:              13976      kB
MemFree:               12168      kB
MemShared:             0          kB
Buffers:               296        kB
Cached:                172        kB
SwapTotal:             0          kB
SwapFree:              0          kB
```

Interface Configuration

```
eth0  Link encap: Ethernet HWaddr 00:DO:CF:00:4D:94
      inet addr: 192.168.1.1 Bcast: 192.168.1.255 Mask: 255.255.255.0
      UP BROADCAST RUNNING MULTICAST MTU: 1500 Metric: 1
      RX packets: 1381 errors: 0 dropped: 0 overruns: 0 frame: 0
      TX packets: 2288 errors: 0 dropped: 0 overruns: 0 carrier: 0
      collisions:3
      Interrupt: 29 Base Address:0x300

eth1  Link encap: Ethernet HWaddr 00:D0:CF:00:4D:95
      inet addr: 172.16.2.231 Bcast: 172.16.2.255 Mask: 255.255.255.0
      UP BROADCAST NOTRAILERS RUNNING MULTICAST MTU:1500 Metric
      RX packets: 43150 errors: 0 dropped: 0 overruns: 0 frame: 0
      TX packets: 13959 errors: 0 dropped: 0 overruns: 0 carrier: 0
      collisions: 1
      Interrupt: 27
```

Figure 25 Device Status Window



```
eth1:0     Link encap: Ethernet HWaddr 00:D0:CF:00:4D:95
           inet addr: 10.120.51.247 P-t-P: 10.120.51.1. Mask:
           255.255.255.255
           UP POINTOPOINT RUNNING MTU: 1400 Metric:1
           RX packets: 77 errors: 0 dropped: 0 overruns: 0 frame: 0
           TX packets: 77 errors: 0 dropped: 0 overruns: 0 carrier: 0
           collisions: 0

lo         Link encap: Local Loopback
           inet addr: 127.0.01 Bcast: 127.255.255.255. Mask: 255.0.0.0
           UP BROADCAST LOOPBACK RUNNING MTU: 3584 Metric:1
           RX packets: 77 errors: 0 dropped: 0 overruns: 0 frame: 0
           TX packets: 77 errors: 0 dropped: 0 overruns: 0 carrier: 0
           collisions: 0
```

Network Devices

```
 Inter–|          Receive                      |          Transmit
 face .| packets  errs   drop   fifo   frame| packers  errs   drop   fifo   colls  carriers
    lo:      77      0      0      0      0        0      0      0      0      0       0
  eth0:    1381      0      0      0      0     2258      0      0      0      0       0
  eth1:   43150      0      0      0      0    13959      0      0      0      1       0
eth1:0     2300      0      0      0      0     1876      0      0      0      0       0
```

Route Table

```
Kernel IP routing table
Destination     Gateway         Genmask          Flags   Metric   Ref   Use:   Iface
192.168.1.0     “               255.255.255.0    U       0        0     32     eth0
172.16.2.0      “               255.255.255.0    U       0        0     5      eth1
127.0.0.0       “               255.0.0.0        U       0        0     1      lo
default         172.16.2.1      0.0.0.0          UG      0        0     0      eth1
```

Interrupts

```
27:             16692           SMC9194
29:             2142            SMC9194
30:             2113573         ColdFire Timer
31:             0               Reset Button
224:            0               ColdRire UART
225:            0               ColdFire UART
```

System Log

```
Wed Apr 11 17:07:45 dhcpcd: got in BOUND state
Wed Apr 11 17:08:32 dhcpd: serving 192.168.1.100
Wed Apr 11 17:12:45  dhcpcd: Time to renew the address...
Wed Apr 11 17:12:45  dhcpcd: Renewing: Send request, timeout=e1, tm=3
Wed Apr 11 17:12:45  dhcpcd: setDhcpInfo ip=3f51410f, lease=258, renew=12c, rebind=20d
Wed Apr 11 17:12:45  dhcpcd: got in BOUND state
Wed Apr 11 17:17:45  dhcpcd: Time to renew the address...
Wed Apr 11 17:17:45  dhcpcd: Renewing: Send request, timeout=e1, tm=3
Wed Apr 11 17:17:45  dhcpcd: setDhcpInfo ip=3f51410f, lease=258, renew=12c, rebind=20d
Wed Apr 11 17:17:45  dhcpcd: got in BOUND state
Wed Apr 11 17:18:32  dhcpd: serving 192.168.1.100
Wed Apr 11 17:18:56  IKE: Trace(*) (IKE) Begin QM Initiator (4409f0) to 146.123.34:500
```

Figure 26 Device Status Window (continued)

Using Advanced Utilities

Advanced Utilities provided by the ANG-1000 include:

- ❒ Setting the MAC Address of a newly attached ANG-1000 when you want to quickly connect to a cable service provider. MAC addresses are used by service providers to identify supported users. The ANG-1000 can proxy your computer's MAC address to the ISP but your provider may require that you change the default value reported by the ANG-1000 to reflect the PC's actual MAC address.
- ❒ Clearing the System Logfile - shown in the Device Status window - when you want to erase old and display updated information.
- ❒ Soft Rebooting to reset the ANG-1000 without recycling power. This function is similar to pressing CTRL-ALT-DELETE on your computer.

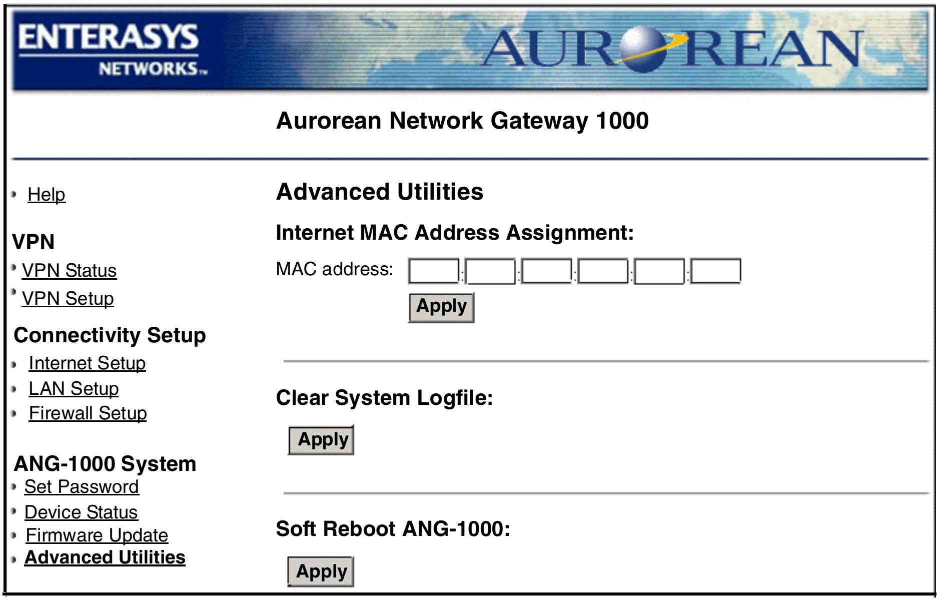


Figure 27 Advanced Utilities Window

1 Click the Advanced Utilities menu option.

The Advanced Utilities window appears as shown in Figure 27.

2 Do one of the following:

- To change the ANG-1000's MAC address to reflect your computer's MAC address, first find the computer's address by issuing the proper command at a DOS prompt. For Windows 95/98/ME systems, type `winipcfg`; for Windows NT/2000 systems, type `ipconfig /all`; for Macintosh systems, check the TCP-IP control panel.

  In the command output, look for the *Physical* or *Adapter Address* value. For example:

  ```
  c:>ipconfig /all
  Ethernet adapter E190x1:

  Description . . : 3Com 3C90x Ethernet Adapter
  Physical Address : 00-10-4B-9D-18-17
  ```

  Enter the value in the **Internet MAC Address Assignment** fields.

  Click Apply and Reboot Now when prompted to save the change.

- Select Clear System Logfile and click Apply.
- Select Soft Reboot ANG-1000 and click Apply.

NOTE

ANG-1000 connections broken during a reboot will be lost after service returns. Idling the traffic stream (Telnet, e.g.) for a couple minutes before re-initiating the connection resolves the problem.

Using the Configuration Editor

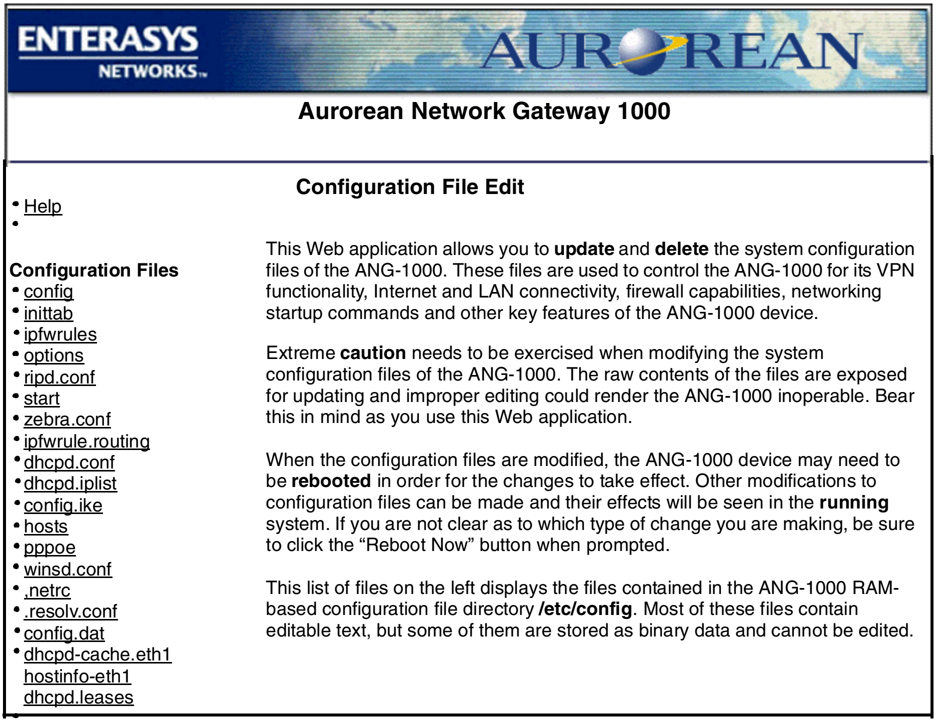
Knowledgeable network administrators can use the Configuration Editor to invoke commands on the ANG-1000's LINUX 2.0 operating system.

CAUTION

Inexperienced users or those unfamiliar with LINUX attempting to use this editor may disable the system. We recommend only expert users, in conjunction with Enterasys Customer Support, use this editor.

1 Click the Configuration Edit menu option.

The Configuration Edit window appears as shown in Figure 28.



Aurorean Network Gateway 1000

Configuration File Edit

- Help
-

Configuration Files

- config
- inittab
- ipfwrules
- options
- ripd.conf
- start
- zebra.conf
- ipfwrule.routing
- dhcpd.conf
- dhcpd.iplist
- config.ike
- hosts
- pppoe
- winsd.conf
- .netrc
- .resolv.conf
- config.dat
- dhcpd-cache.eth1 hostinfo-eth1 dhcpd.leases

This Web application allows you to **update** and **delete** the system configuration files of the ANG-1000. These files are used to control the ANG-1000 for its VPN functionality, Internet and LAN connectivity, firewall capabilities, networking startup commands and other key features of the ANG-1000 device.

Extreme **caution** needs to be exercised when modifying the system configuration files of the ANG-1000. The raw contents of the files are exposed for updating and improper editing could render the ANG-1000 inoperable. Bear this in mind as you use this Web application.

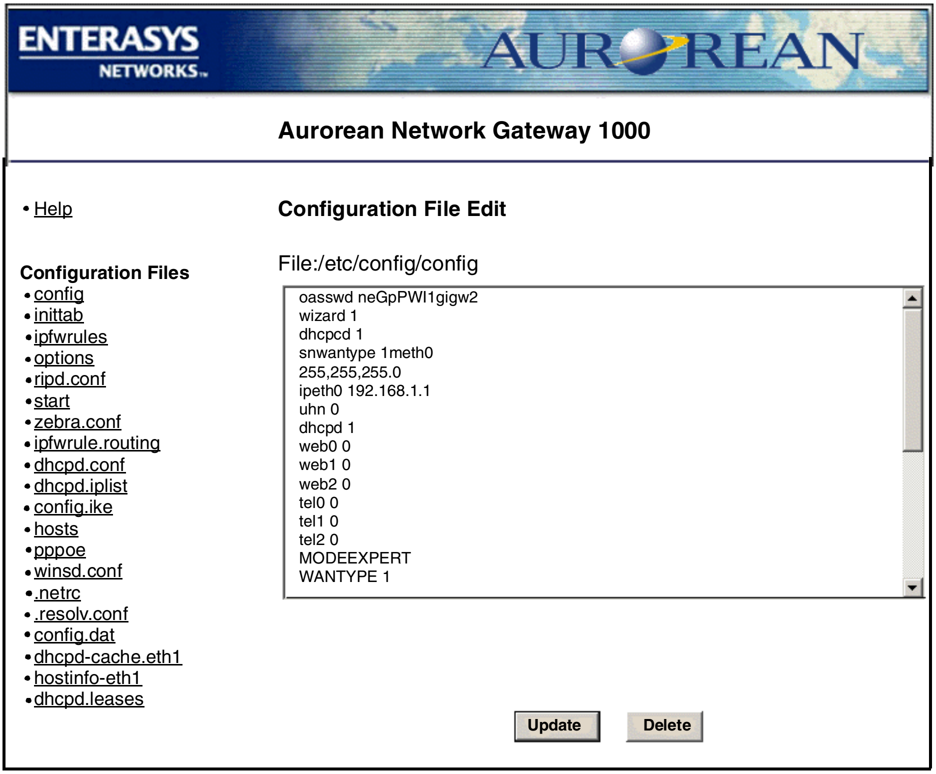
When the configuration files are modified, the ANG-1000 device may need to be **rebooted** in order for the changes to take effect. Other modifications to configuration files can be made and their effects will be seen in the **running** system. If you are not clear as to which type of change you are making, be sure to click the "Reboot Now" button when prompted.

This list of files on the left displays the files contained in the ANG-1000 RAM-based configuration file directory **/etc/config**. Most of these files contain editable text, but some of them are stored as binary data and cannot be edited.

Figure 28 Configuration Edit Window

2 Click on the command of your choice.

3 The arguments of the command you selected are displayed in the Configuration File Edit window, as shown in Figure 29.



File:/etc/config/config

```
oasswd neGpPWI1gigw2
wizard 1
dhcpcd 1
snwantype 1meth0
255,255,255.0
ipeth0 192.168.1.1
uhn 0
dhcpd 1
web0 0
web1 0
web2 0
tel0 0
tel1 0
tel2 0
MODEEXPERT
WANTYPE 1
```

Figure 29 Configuration File Edit Window

4 Edit the UNIX command and click Update or Delete.

NOTE

You can remove the Configuration Editor (along with the Advanced Utilities option) from the main menu by selecting the *config* command, deleting the **MODEEXPERT on** argument and clicking Update.

NOTE

If you press the reset button after you have configured your ANG-1000, you will lose your entire configuration. Any settings you have changed from factory defaults, such as firewall rules, will be removed. We recommend that you save these settings to a Notepad file which you then can reference if you are compelled to use the reset button.

Configuring IP Port Forwarding

ANG-1000's support of IP Port Forwarding permits you to make servers on the trusted network of the ANG-1000 available to the rest of the VPN. In contrast to Network Address Translation (NAT), which allows access to external-side servers initiated by *internal-side* hosts, Port Forwarding permits access to internal-side servers initiated by external-side hosts.

This is accomplished by rewriting the headers of all packets bound for the ANG-1000 and forwarding them to another host on the trusted-side of the network, depending on their destination port (port numbers corresponding to standard, well-known protocols). The IP addresses are re-written so that incoming IP (TCP and UDP) packets are forwarded to their intended destinations, and the reply packets are re-written to appear to be coming from the ANG-1000.

This process requires static, known values for the following:

- The *IP address assigned to ANG-1000* by the VPN. This address is in RiverMaster in the ANG-1000's user account and may not be assigned dynamically via pools or virtual subnets.
- The *IP address of the server* on the ANG-1000 trusted network (one server per protocol). This may not be dynamically assigned by the ANG-1000 via DHCP.
- The *protocol* (TCP or UDP) and the *protocol port number.*

IP Port Forwarding is configured by editing the *ipportfw* command in the *ipfwrules* configuration file in the Config Editor tool of the Web Config. The ipportfw commands should be entered at the end of the ipfwrules file.

Refer to the tables below for command usage, switches, arguments, and definitions.

Usage		
ipportfw -A -[t | u] l.l.l.l/lport -R a.a.a.a/rport		add entry
ipportfw -D -[t | u] l.l.l.l/lport		delete entry
	l.l.l.l is the address of the VPN interface receiving packets to be forwarded	
	a.a.a.a is the server address on the LAN	
	lport is the port being redirected	
	rport is the port being redirected to	

Switch	<arg>	Definition
-t	VPN address/port	Forward TCP traffic
-u	VPN address/port	Forward UDP traffic
-A	None	Add the IP port forwarding table entry
-C	None	Clear the IP port forwarding table
-D	None	Delete the IP port forwarding table entry
-R	IP address/port	Define the server IP address
-L	None	List the IP port forwarding table

Follow the steps below to configure IP port forwarding.

1. Login to Web Config.
2. Click on the Config File Editor menu option.
3. Click on the ipfwrules Configuration File.
4. In the Configuration File Edit window, scroll to the end of the file.
5. Under **Expert-Config**, type the following rules:
   - ipportfw -C
   - ipportfw -A <-t or -u> <VPN address/local port> -R <local server IP address/remote port>
6. Click Update and Reboot Now when prompted to save the change.

Refer to the table below for a sample IP port forwarding configuration:

Example

```
ipportfw -C
ipportfw -A -t10.120.50.215/23 -R 192.168.0.1/23
ipportfw -A -t10.120.50.215/21 -R 192.168.0.1/21
ipportfw -A -t10.120.50.215/6000 -R 192.168.0.2/6000
```

The above sample configuration performs the following tasks:

❒ Clears the IP port forwarding table

❒ Maps telnet (TCP port 23) from the VPN address (10.120.50.215) to port 23 on the internal server 192.168.0.1

❒ Maps FTP from the VPN address to the same 192.168.0.1 server

❒ Maps X windows (TCP port 6000) to a different server, 192.168.0.2

A

Glossary

Aurorean Network Gateway

An Enterasys Networks device that creates a secure virtual private circuit over the Internet between itself and a remote user′s computer. The Aurorean Network Gateway encapsulates data packets using **IPSec** and encrypts data to prevent third-parties from intercepting and examining it. There are three types of Aurorean Network Gateways:

- ❒ Aurorean Network Gateway-7000 - a tunnel server that can accommodate up to 5000 remote users
- ❒ Aurorean Network Gateway-3000 - a tunnel server that can accommodate up to 500 remote users
- ❒ Aurorean Network Gateway-1000 - a tunnel server that establishes a site-to-site tunnel between itself and either an ANG-7000 or an ANG-3000 server. It can accommodate up to 25 tunnels.

Aurorean Web Config

Aurorean Web Config is the utility used to configure the Aurorean Network Gateway-1000. It is Web based and is accessed through the use of a Web browser.

Aurorean Policy Server

An Enterasys Networks device that manages **Aurorean Network Gateways**. Network administrators configure Aurorean Policy Servers from a RiverMaster computer. The network administrator can create a remote user database on the Aurorean Policy Server or instruct the **Aurorean Policy Server** to authenticate remote users against an external authentication server (such as a RADIUS or SecurID server). When the network administrator changes tunnel connection parameters, the Aurorean Policy Server provide updated configuration files to Aurorean Network Gateways on request.

DHCP

Dynamic Host Configuration Protocol (DHCP) servers are used to assign IP addresses. The Aurorean Network Gateway-1000 is capable of assigning IP addresses.

DSL

Refers to Digital Subscriber Lines. DSL technologies use sophisticated modulation schemes to pack data onto copper wires. They are sometimes referred to as last-mile technologies because they are used only for connections from a telephone switching station to a home or office, not between switching stations. Usually the maximum distance between the home or office and the switching station has to be around one mile.

Ethernet

The Ethernet originated in 1974 by Xerox to connect many office machines together to allow communications between them. Coax cable was originally used. today twisted pair wire can be used and the speeds can be up to 10 megabits per second.

Firewall

A combination of hardware and software which limits the exposure of a corporate network to outside attack by enforcing a boundary between the network and the Internet. Firewalls normally fall into one of two categories: application-level or network-level (often referred to as a packet filter). An application-level firewall examines traffic at the application level, and only passes packets that are sent by approved applications (such as FTP, E-mail, or Telnet). This type of firewall often readdresses outgoing traffic so that it appears to have originated at the firewall rather than an internal host, thereby concealing the address of the internal host. A network-level firewall examines traffic at the network packet level, and filters packets based on the destination and/or source address.

Generic Routing Encapsulation (GRE)

Tunneling protocol developed by Cisco that can encapsulate a wide variety of protocol packet types inside IP tunnels, creating a virtual point-to-point link over the Internet. For **PPTP**, **GRE** is used to encapsulate **PPP** data packets within an IP packet (IP packet headers contain address information necessary for routing, while PPP packets do not).

Internet Service Provider (ISP)

A vendor who provides direct access to the Internet. ISPs bill users for the amount of time they are connected, and may also offer additional services such as Web site hosting, E-mail, or news group readers. Remote users reach the ISP by dialing into an ISP **POP** with a computer, modem, and phone line, or over a dedicated circuit (such as a cable modem connection).

IP

Abbreviation of *Internet Protocol*, pronounced as two separate letters. IP specifies the format of packets, also called datagrams, and the addressing scheme. Most networks combine IP with a higher-level protocol called *Transport Control Protocol (TCP/IP)*, which establishes a virtual connection between a destination and a source.

IP Address

An identifier for a computer or device on a TCP/IP network. Networks using the TCP/IP protocol route messages based on the IP address of the destination. The format of an IP address is a 32-bit numeric address written as four numbers separated by periods. Each number can be zero to 255. For example, 172.16.4.14 could be an IP address.

IP Security Protocol (IPSec)

Short for *IPSecurity*, a set of protocols developed to support secure exchange of packets at the IP layer.

LAN

Locan Area Network (LAN) connects computers and peripherals together in an office or a campus to allow the computers to access each other and other common peripherals.

LEDs

Abbreviation of *light emitting diode*, an electronic device that lights up when electricity is passed through it. LEDs are usually red, but the ANG-1000 uses green LEDs. The LEDs are used to indicators.

Mac Address

Short for *Media Access Control address*, a hardware address that uniquely identifies each node on a network.

Network Address Translation (NAT)

Described by Whatis.com as the translation of an Internet Protocol address used within one network to a different IP address known within another network. One network is designated the inside network and the other is the outside. Typically, a company maps its local inside network addresses to one or more global outside IP addresses and unmaps the global IP addresses on incoming packets back into local IP addresses. This provides security since each outgoing or incoming request must undergo a translation process that also offers the chance to qualify or authenticate the request or match it with a previous request. **NAT** also conserves the number of global IP addresses that a company uses and permits the use of a single IP address to interface with the world. **RiverMaster** permits the **Aurorean Network Gateway** to be configured as a **NAT server**.

Network Administrator

The person responsible for installing and maintaining a company's network equipment, and also insuring that network resources (such as servers and the applications running on them) are consistently available and performing well. In terms of Enterasys Networks products, this person physically installs **Aurorean Policy Servers** and **Aurorean Network Gateways**, distributes **Aurorean Client Software** to **remote users**, and runs **RiverMaster** software on his/her computer to manage the entire **VPN**.

Point of Presence (POP)

In Internet terms, the physical site that contains an **ISP's** network equipment. Remote users dial into the POP, authenticate against the ISP's customer database, and then gain access to the Internet. ISPs typically have POPs scattered throughout their service area, so that can customers can dial a local phone call and avoid paying long- distance charges when accessing the Internet.

Point-to-Point Protocol (PPP)

The Internet standard for sending network traffic over serial lines, such as dial-up phone lines. Unlike its predecessor SLIP (Serial Line Internet Protocol), PPP provides error detection and compression capabilities.

Point-to-Point Tunneling Protocol (PPTP)

A network protocol for linking remote locations over the Internet rather than over costly long-distance or leased lines. To accomplish this, PPTP encapsulates other network protocols (such as TCP/IP, IPX, and NetBEUI) and uses encryption to secure the data sent over the Internet. PPTP was developed jointly by Microsoft and U.S. Robotics (3Com).

PPPoE

The *Point-to-Point over Ethernet* protocol provides a connection to the Internet through a DSL provider. It is also identified as *PPPoE*.

RiverMaster

A management application running on a Windows NT 4.0 Workstation computer which communicates with **Aurorean Policy Servers** and **Aurorean Network Gateways**. Using RiverMaster, a **network administrator** creates user databases, sets policies for user groups, views activity logs, and generates usage reports.

Routers

Devices which direct network traffic among LANs or WANs until the data reaches its destination. To do this, routers communicate with one another using dedicated protocols such as IGRP (Interior Gateway Routing Protocol) and BGP (Border Gateway Protocol) to transfer information on network addressing, status, and configuration.

TCP/IP

Abbreviation for *Transmission Control Protocol/Internet Protocol.* The suite of communications protocols used to connect hosts on the Internet. TCP/IP uses several protocols, the two main ones being TCP and IP. TCP/IP is built into the UNIX operating system and is used by the Internet, making it the de facto standard for transmitting data over networks. Even network operating systems that have their own protocols, such as Netware, also support TCP/IP.

Tunneling

Technology that lets a network transport protocol carry information for other protocols within its own packets. For example, by encapsulating NetBEUI packets, IP can route them across the Internet, which is not normally possible.

Virtual Private Network (VPN)

An extension of a company’s private network that uses the resources of the public Internet. While most private networks use dedicated lines and equipment that are company property, a virtual private network “borrows” resources from the Internet on an as-needed basis.

B

Specifications

This appendix details the specifications of the ANG-1000.

Table 1 ANG-1000 Specifications

Category		**Parameters**
Chassis	Depth	6 1/2”
	Width	10”
	Height	1 /7/8”
	Weight	1 lb.
Environment	Operating Temperature	0° to 70° C
PFC Power Supply	Power Adapter	Input: 100-240VAC, ~0.4A, 47-63Hz Regulated UL Listed Class 2 power supply must be used.
		Output: 5v VDC, 2.5 Amp
CPU	Processor	Motorola© Coldfire XCF5307 91.5 Mhz
	Memory	16 MB DRAM
Storage Devices	Hard Drive	2 MB Flash
Performance	Server Capacity	> 25 concurrent tunnels
	Tunnel Performance	Up to 3 Mbps with IPSec

Table 1 ANG-1000 Specifications (Continued)

Category		**Parameters**
Protocols & Standards	Tunnel Protocols	IP Security Protocol (IPSec) as defined in RFC 2401 and 2409 Point-to-Point Tunneling Protocol (PPTP) as defined in RFC 1234 Generic Routing Encapsulation (GRE) as defined in RFC 1701 and 1702
	Encapsulated LAN Protocols	IP
	Routing Protocols	RIP V1, V2 Support for dynamic Virtual Network addressing, local network addressing, or static routes
	Authentication	Challenge Handshake Authentication Protocol (CHAP) MS-CHAP (Microsoft proprietary version of CHAP)
	Encryption	MPPE, 40-bit and 128-bit configurable keys (RC4-compatible) DES (56-bit) or Triple-DES (168-bit) with IPSec only
	Compression	Microsoft Point-to-Point Compression (MPPC)
Ethernet	Number of Ports	Two
	Data Transfer Rate	10 Mbps
	Connector	8-position modular jack (RJ-45)
Safety Regulations	US/Canada/ Europe	UL 1950, CSA C22.2 No.950, 73/23/EEC, EN60950, and IEC950
EMCI	US, Canada, Europe, Japan, Australia, New Zealand, Taiwan, Russia, International	FCC Part 15, CSA C108.8, 89/336/EEC, EN55022, EN61000-3-2, EN61000-3-3, EN50082-1, AS/NZS3548, and VCCI VD3. この装置は，情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

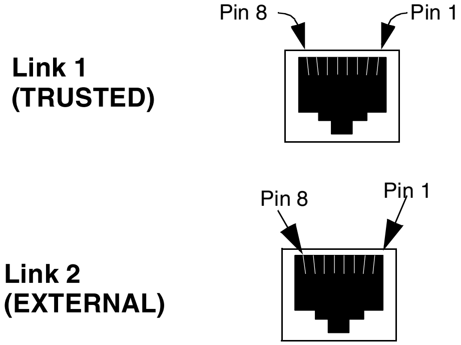
C

Pin Assignments

This appendix describes pin assignments for the Ethernet connectors on the back of the ANG-1000. Because ANG-1000 servers ship with all the cables required, this information is only necessary if you need to purchase or fabricate a replacement cable.

ANG-1000 servers are equipped with Ethernet ports located at the rear of the chassis, supporting full-duplex 10Base-T transmission.

Both port types conform to IEEE 802.3 standards with 8-pin modular RJ-45 connectors. Figure 2 shows the pin assignments for ANG-1000 server Ethernet ports.



Pin	Signal
1	Transmit +
2	Transmit -
3	Receive +
4	*Return*
5	*Return*
6	Receive -
7	*Return*
8	*Return*

Figure 1

Figure 2 Ethernet Port Pin Assignments

Replacement Ethernet cables must meet the following requirements:

❒ Category 3, 4, or 5 unshielded twisted-pair (UTP) wiring

❒ Length cannot exceed 328 feet (100 meters)

D

License Agreement & Support

This appendix describes the terms and conditions that govern the use of Aurorean Virtual Network products (including the warranties) and provides contact information for obtaining technical support from Enterasys Networks.

Enterasys Networks License Agreement

PLEASE READ THIS DOCUMENT CAREFULLY BEFORE USING ENTERASYS SOFTWARE. BY USING THE SOFTWARE PRODUCT SHIPPED TO YOU BY ENTERASYS OR ITS DISTRIBUTOR ("LICENSED SOFTWARE") YOU ACCEPT THE TERMS OF THIS SOFTWARE LICENSE AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, DO NOT USE THE SOFTWARE PRODUCT. YOU MAY RETURN THIS PRODUCT TO ENTERASYS FOR A FULL REFUND.

The Licensed Software is licensed, not sold, to you for use only under the terms of this license, which represents the complete agreement and understanding between you and Enterasys. Enterasys reserves any rights not expressly granted to you. You own the media on which the software is originally or subsequently recorded or fixed, but Enterasys retains ownership of all copies of the software itself.

License Grant

Enterasys Networks, Inc., 35 Industrial Way, Rochester, New Hampshire 03866 hereby grants to Licensee a personal, nonexclusive, non-transferable license to use the Licensed Software on the servers on which the Software is first installed ("Licensed Servers") and on an unlimited number of client processors, subject to the limit on simultaneous users as specified by the scope of the license that Licensee has purchased from Enterasys. Should one or more the above Licensed Servers be upgraded and/or replaced by other Enterasys servers purchased by Customer pursuant to Enterasys' then current upgrade policy, the license may be transferred and the Software may be used on the replacement server(s). This License shall commence upon the receipt by Licensee of the Licensed Software and shall continue until Licensee discontinues use or this Agreement is terminated. No ownership of the Licensed Software or any of its parts is transferred to Licensee.

Licensee may make copies of the Licensed Software in object code form for archival and backup purposes only. All copies (including copies of the documentation) must bear the copyright notice(s) and restricted rights legend contained in or on the original.

Except as expressly permitted by law without the possibility of contractual waiver, Licensee agrees that it will not attempt to reverse engineer, reverse compile or reverse assemble the Licensed Software or otherwise seek to gain access to source code for the Licensed Software.

Licensee shall take all reasonable steps to protect the Licensed Software and documentation from unauthorized copying and use. Licensee shall not, without the express written consent of Enterasys, provide, disclose, transfer or otherwise make available any Licensed Software, or copies thereof, to any third party.

Warranty

Enterasys warrants to Licensee that the Licensed Software will, when used in the specified operating environment, substantially perform in the manner described in its documentation, as it exists at the date of delivery, for a period of one year from the date of original delivery to the Licensee. Enterasys's sole obligation under this warranty shall be limited to using reasonable efforts to correct reproducible defects and distribute such corrections as part of the next scheduled maintenance release of the Software. Enterasys does not warrant that: (i) operation of any of the Licensed Software will be uninterrupted or error free, or (ii) functions contained in the Licensed Software shall operate in the combination which may be selected for use by Licensee or meet Licensee's requirements. Enterasys's warranty obligations shall be void if the Licensed Software is modified without the written consent of Enterasys.

EXCEPT AS SPECIFICALLY PROVIDED HEREIN, THERE ARE NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY IMPLIED WARRANTY OF MERCHANTABILITY OR ANY IMPLIED WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE.

Infringement Indemnification

Enterasys shall indemnify, defend and hold Customer harmless from and against any claims, actions, or demands alleging that the Licensed Software directly infringes any United States patent, trademark, or copyright, or misappropriates any trade secret right of any third party, provided that Customer promptly notifies Enterasys of any such claim, allows Enterasys to control the defense and provides reasonable information and assistance to Enterasys (at Enterasys' expense) in the defense of the claim. Customer shall permit Enterasys to replace or modify any affected Licensed Software to avoid infringement, or to procure for Customer the right to continue to use such Licensed Software. If neither of such alternatives is reasonably possible, Enterasys may require Customer to return the affected Licensed Software to Enterasys and Enterasys' sole liability in regard to such return shall be to refund the purchase price paid by Customer. Enterasys shall have no obligation with respect to claims, actions, or demands to the extent that they are based upon (i) the combination of Licensed Software with any items not supplied by Enterasys, (ii) any modification or change to the Licensed Software by Customer, or, (iii) any failure by Customer to implement modifications or replacements distributed by Enterasys that address any alleged infringement. This Section states the entire liability of Enterasys with respect to indemnification or liability for infringement or misappropriation of patents, copyrights, trademarks, trade secrets or other proprietary rights by Enterasys or the Licensed Software or any part thereof or by their use or operation.

Limitation of Liability

ENTERASYS AND ITS LICENSORS' TOTAL LIABILITY FOR ANY CAUSE OF ACTION ARISING IN CONNECTION WITH THIS AGREEMENT, AND REGARDLESS OF THE FORM OF ACTION, WHETHER IN CONTRACT OR IN TORT INCLUDING NEGLIGENCE, SHALL BE LIMITED TO THE ACTUAL DOLLAR AMOUNT ENTERASYS RECEIVED HEREUNDER FROM CUSTOMER FOR THE PARTICULAR PRODUCTS WHICH ARE THE

SUBJECT MATTER OF THE CAUSE OF ACTION. IN NO EVENT SHALL ENTERASYS BE LIABLE FOR ANY LOST OR ANTICIPATED PROFITS OR SAVINGS, OR ANY INCIDENTAL, EXEMPLARY, PUNITIVE, SPECIAL OR CONSEQUENTIAL DAMAGES, REGARDLESS OF THE FORM OF ACTION, WHETHER IN CONTRACT OR IN TORT INCLUDING NEGLIGENCE, AND WHETHER OR NOT ENTERASYS WAS ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

SOME STATES DO NOT PERMIT DISCLAIMERS OF IMPLIED WARRANTIES OR OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, SO THE ABOVE DISCLAIMERS MAY NOT APPLY TO YOU.

Termination

Enterasys may terminate this license agreement and Licensee's right to use the Licensed Software if Licensee materially breaches the terms of this Agreement or fails to pay the licensee fee when due, and fails to cure such breach within thirty days of notice thereof by Enterasys.

International Provisions

Licensee agrees that it shall not directly or indirectly export the Licensed Software, individually or as part of a system, without first obtaining a license from the U.S. Department of Commerce or any other appropriate agency of the U.S. Government, as required. Diversion of products contrary to U.S. law is prohibited.

Applicable Law

The parties agree that this license shall be governed by the substantive laws of the Commonwealth of Massachusetts and the United States. The exclusive jurisdiction for any dispute regarding this Agreement shall be in the United States of America or, for Licensees located in Europe, London, England. The parties expressly disclaim the applicability of the U.N. Convention on the Sales of Goods.

U. S. Government - Commercial Computer Software

This Licensed Software is Commercial Computer Software as provided in 48 CFR 2.101 and is licensed to U.S. Government agencies and personnel only with the rights set forth in this license. The use of the Licensed Software by the Government constitutes acknowledgment of Enterasys's proprietary rights in the Licensed Software. The manufacturer is Enterasys Networks, 35 Industrial Way, Rochester, New Hampshire 03866. The licensee or user of this product agrees not to remove any of the RESTRICTED RIGHTS legends and markings included in this software and associated documentation.

Technical Support

Enterasys Networks provides easy access to technical support information through a variety of services.

Support from Enterasys Networks

Enterasys Networks offers two ways of contacting customer support personnel.

On-line Services

To receive answers to technical questions on Aurorean Virtual Network products, send E-mail to:

`support@enterasys.com`

Please include your name, title, company, and phone number in all correspondence.

Phone Support

Enterasys Networks customer support personnel are available by calling **1-800-872-8440**. When you call, please call from a position where you can operate the RiverMaster management application or view the server's LEDs, and make sure you have the following information ready:

❒ State of the LEDs on both the front and rear panels of the server(s)

❒ A list of the error messages appearing in the RiverMaster message/alarm display

❒ Details about any recent configuration changes, if applicable

Enterasys Networks also recommends that you have the *RiverMaster Administrator's Guide* on hand when you call.

Returning Products for Repair

After discussing the problem with Enterasys Networks Customer Support or your authorized Enterasys Networks reseller, you may be asked to return the APS-3000/7000 or ANG-1000/3000/7000 for repairs. You will receive a Return Material Authorization (RMA) number for the server. Ship the server, with the RMA number clearly visible on the outside of the package, to the following address:

Enterasys Networks
35 Industrial Way
Rochester, NH 03866

Enterasys Networks recommends that you reuse the original shipping box or equivalent packaging to protect the server during shipment.

NOTE

Products sent to Enterasys Networks without an RMA number will be returned to the sender unopened, at the sender's expense.

Index